Xournals

Academic Journal of Computer Sciences

ISSN UA | Volume 01 | Issue 01 | June-2018

A Study on Preventive Methods used for Distributed Denial of Service Attacks

Vaivbhav Tyagi[1] and Umakant Dwivedi[1]

Available online at: www.xournals.com

Received 14th January 2018 | Revised 18th April 2018 | Accepted 25th May 2018

Abstract:

In today's scenario, Denial of Service (DoS) has become an extortion weapon and casing damage to multiple internet user. DDoS attacks rates are increasing in an exponential style and a report showed that DDoS attack rate is 300GB per second. In 2000, very famous CNN, Amazon and Yahoo, also became the targets of DDoS attacks and it's an alarming sign that DDoS attacks rate will definitely increase in coming year. To overcome with this problem numerous preventive techniques has been proposed. Here in this paper, an effort has been done on the recent preventive techniques used for Distributed Denial of Service (DDoS) attacks as internet security has always been a concern for internet user.

Keywords: *DoS, DDoS, Preventive Techniques for DDoS,*

Authors:

1. *Department of Information Technology, Bharat Institute of Technology, Meerut, Uttar Pradesh Technical University, INDIA*

Introduction

In current scenario, internet has become a significant part of our society in different ways due to which cyberspace attacks has also been increased. For instance, Denial of Service, Information Phishing, Financial Fraud, Email Spamming etc. Among numerous internet based attacks Denial of Service is one of the very critical and continuous threat in the world of cyber security. Denial-Of-Service is an attack targeted at divesting genuine users from online services, it is caused by overflowing the network or server with invalid authentication requests which ultimately down the server or network. And when the DoS attacks are organized by multiple distributed computers, it is commonly known as distributed denial of service DDoS attack. DDoS attack is one of the most popular attack in the world of cyber and the targets are Routers, Links, Firewalls and defense systems, Victim's Infrastructure, Victim's OS, Current Communication, and Victim's Application. Basically there three types of DDoS attacks i.e. Network-centric or volumetric attacks, protocol attacks target network layer or transport layer protocols and application layer attacks. The inundation of packets at the target causes a denial of service. In 1988, only six DDoS attack were recorded but the number of attacks increasing day by day.

Basically there are two type of DDoS attacks i.e. typical DDoS attack (shown in figure 1) and DRDoS (Distributed Reflection Denial of Service) attack (shown in figure 2) and both types are compromised machines which have been recruited during the scanning process and are installed with malicious code. Below figure 1 shows the typical DDoS attack (Yu, 1; https://economictimes.indiatimes.com; Bhattacharyya and Kalita, 5; https://searchsecurity.techtarget.com).

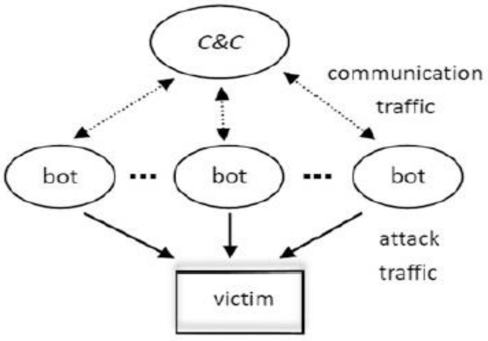

Figure 1: A typical DDoS attack

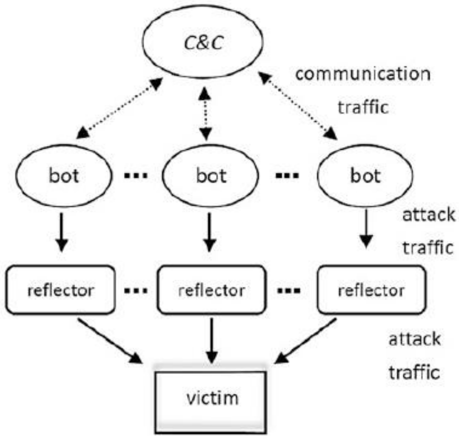

Figure 2: A DRDoS Attack

Causes

DDoS attacks are disastrous and bring down a server or network very easily and rapidly. Following are different reasons for DDoS attacks:

- High interdependencies exist in Internet security.
- Inadequate internet resources.
- Several unintentionally compromised hosts, plot against a few target servers of hosts.
- Many a time intelligence and resources are used to prevent impending attacks which are not usually collected.
- On internet straightforward routing principles are used.
- There are mismatches in design and speeds between core and edge networks are commonplace.
- Slack network management.
- Common and useful practice of sharing resources has its drawbacks (Bhattacharyya and Kalita, 4, 5).
- Every cultural heritage has its own interesting and important story.

A Case Study: For Example

In 2015, Rio Olympics suffered from DDoS attack, a campaign used a DDoS-for-hire service called LizardStresser for launching attack traffic against their targets. As the games came closer, LizardStresser along with several other Internet of Things (IoT) botnets attacked at 540 Gbps. This could have been easily disrupted the media coverage of the Rio Olympics but thanks to the mitigation measures provided by Arbor Networks, Brazilian information security professionals and the International Olympics Committee (IOC) kept their systems up running (https://www.tripwire.com).

Review of Literature

Kim *et al.* (2004), proposed a combined data mining approach for the DDoS attack detection of the various types, which is composed of the automatic feature selection module by decision tree algorithm and the classifier generation module by neural network.

Elleithy *et al.* (2006), in their paper discussed about the implementation and analysis of three main types of attack: Ping of Death, TCP SYN Flood, and Distributed DoS. In this paper they demonstrated the potential damage from DoS attacks and analyze the consequences of the damage.

Hussain *et al.* (2006), proposed an attack fingerprinting system to identify repeated DDoS attack. In this paper they concluded that their system provides a new tool that can be used to assist in criminal and civil prosecution of the attackers which will enhance network traffic forensic capabilities and aid in investigating.

Lu *et al.* (2007), proposed a novel framework to robustly and efficiently detect DDoS attacks and identify attack packets with an aim to exploit spatial and temporal correlation of DDoS attack traffic. They had design a perimeter-based anti-DDoS system, in which traffic is analyzed only at the edge routers of an ISP network.

Gupta *et al.* (2008), proposed novel framework that deals with the detection of variety of DDoS attacks by monitoring propagation of abrupt traffic changes inside ISP Domain and then characterizes flows that carry attack traffic. They have shown simulation results that, our novel framework can effectively detect and characterize different kinds of DDoS attacks.

Yu and Zhou (2008), focused on detection of DDoS attacks in community networks through Entropy-Based Collaborative Detection Method. In which they calculated flow of entropy, they found that if the router entropy is less than a given threshold, then a attack alarm is raised; the routers on the path of the suspected flow will calculate the entropy rate of the suspected flow. If the entropy rates are the same or the difference is less than a given value, then we can confirm that it is an attack, otherwise, it is a surge of legitimate accessing. In their paper they proved that combine the router entropy and the entropy rate of flows, we can discriminate DDoS attacks from surge legitimate accessing, moreover, we can identify attacks at the early stage.

Kumarasamy (2011), proposed a method which provides the strong defense against DDoS attacks. It very easily recognizes the attacker hosts by their traffic nature and blocks all the traffic from the attacker hosts. With the help of this method the attacker traffic is effectively blocked and can be identified at very initial step.

Priyadharshini1 and Kuppusamy (2012), in their paper proposed a new cracking algorithm to stop that DDoS attacks. This proposed algorithm was made user friendly domain and have the capability of segregating the clients from the attackers by posting requests for unnecessary reasons. Their basic idea behind the proposal is to protect the server or network from DDoS attacks. This new cracking algorithm effectively gives the availability of web services during DDoS attack.

François *et al.* (2012), proposed FireCol to overcome with the problem of DDoS attacks. It is scalable solution for primary detection of DDoS attacks and composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. FireCol gave good result and highlighted good practices for its configuration, FireCol can be extended in future to support different IPS rule structures.

Bhange *et al.* (2012), discussed about the statistical approach about the DDoS Attacks and their impact on network traffic. They also discussed about the EM algorism for estimating the distribution parameter of Gaussian mixture distribution model and a method to recognize anomalies in network traffic.

Devi and Yogesh (2012), proposed an effective and efficient defense scheme against DDoS attacks based on information metric (entropy). This methods basically provides a double check point for detection of malicious flow from the normal flow.

Mahajan and Sachdeva (2013), focus mainly on the DDoS attack which hampers the network or server availability. They also discussed the different techniques which are used to prevent and mitigate these attacks with their advantage and disadvantage. Different prevent and mitigation techniques are Ingress Filtering, Egress Filtering, Route Based Distributed Packet Filtering, History Based IP-Filtering, Secure Overlay Services (SOS), Load Balancing and Honey pot; Integrated Intserv, Differentiated Services, Class Based Queuing, Resource Pricing, PushBack, Throttling respectively. Above all the attacks are still one of the major issue for which they suggested that different effective methods can be used to prevent oneself from DDoS attack.

Zlomislić *et al.* (2017), presents a review of current denial of service (DoS) attack and defence concepts, from a theoretical and practical point of view and proposed for future research.

Conclusion

According to the review study, it has been concluded the inspite of several preventive of DoS attack, there are still many insecure machines over the internet that can be launch large-scale DDoS attacks. Therefore, in this paper we covered different preventive techniques used for the protection from DDoS attack, which provide better understanding about DDoS attacks. For more protection from DDoS attacl researchers have to effectively work to develop a comprehensive solution that encompasses several defense activities to trap variety of DDoS attack.

References:

Yu, Shui. *Distributed Denial of Service Attack and Defense*. Springer, 2014.

"Definition of Denial-of-Service Attack | What Is Denial-of-Service Attack? Denial-of-Service Attack Meaning." *The Economic Times*, Economic Times, Available at: economictimes.indiatimes.com/definition/denial-of-service-attack.

"What Is Distributed Denial of Service (DDoS) Attack? - Definition from WhatIs.com." *SearchSecurity*, TechTarget, Available at: https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.

Bhattacharyya, Dhruba Kumar, and Jugal Kumar Kalita. *DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance*. CRC Press, 2016.

Mahajan, Deepika, and Monika Sachdeva. "DDoS Attack Prevention and Mitigation Techniques - A Review." *International Journal of Computer Applications*, vol. 67, no. 19, 2013, pp. 21–24.

Priyadharshini, V., and K. Kuppusamy. "Prevention of DDOS Attacks Using New Cracking Algorithm." *International Journal of Engineering Research and Applications (IJERA) I*, vol. 2, no. 3, 2012, pp. 2263–2267.

Elleithy, Khaled M., et al. "Denial of Service Attack Techniques: Analysis, Implementation and Comparison." *Research Gate*, Available at: www.researchgate.net/profile/Khaled_Elleithy/publication/242497142_Denial_of_Service_Attack_Techniques_Analysis_Implementation_and_Comparison/links/0deec522bc76abe6d7000000/Denial-of-Service-Attack-Techniques-Analysis-Implementation-and-Comparison.pdf

Francois, Jérôme, et al. "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks." *IEEE/ACM Transactions on Networking*, vol. 20, no. 6, 2012, pp. 1828–1841.

Gupta, B. B., et al. "An ISP Level Solution to Combat DDoS Attacks Using Combined Statistical Based Approach ." *Journal of Information Assurance and Security* , vol. 2, 2 June 2008, pp. 102–110.

Yu, Shui, and Wanlei Zhou. "Entropy-Based Collaborative Detection of DDOS Attacks on Community Networks." *2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2008.

Kim, Mihui, et al. "A Combined Data Mining Approach for DDoS Attack Detection." *Lecture Notes in Computer Science Information Networking. Networking Technologies for Broadband and Mobile Networks*, 2004, pp. 943–950.

References:

Lu, Kejie, et al. “Robust and Efficient Detection of DDoS Attacks for Large-Scale Internet.” *Computer Networks*, vol. 51, no. 18, 2007, pp. 5036–5056.

Bhange, Anup, et al. “DDoS Attacks Impact on Network Traffic and Its Detection Approach.” *International Journal of Computer Applications*, vol. 40, no. 11, 2012, pp. 36–40.

Kumarasamy, Saravanan. “Distributed Denial of Service (DDOS) Attacks Detection Mechanism.” *International Journal of Computer Science, Engineering and Information Technology*, vol. 1, no. 5, 2011, pp. 39–49.

Devi, S Renuka. “Detection of Application Layer DDOS Attacks Using Information Theory Based Metrics.” *Computer Science & Information Technology (CS & IT)*, 2012.

DMBisson, David BissonFollow. “The 5 Most Significant DDoS Attacks of 2016.” *The State of Security*, 29 Nov. 2016, Available at: www.tripwire.com/state-of-security/security-data-protection/cyber-security/5-significant-ddos-attacks-2016/.

Hussain, A., et al. “Identification of Repeated Denial of Service Attacks.” *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, 2006.

Zlomislić, Vinko, et al. “Denial of Service Attacks, Defences and Research Challenges.” *Cluster Computing*, vol. 20, no. 1, 2017, pp. 661–671.