Xournals

Academic Journal of Computer Sciences

ISSN UA | Volume 01 | Issue 01 | January-2019

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 10th September 2018 | Revised 27th October 2018 | Accepted 28th December 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 represented rate of DDoS attack i.e. 300GB per second. In 2000, very famous Amazon, Yahoo and CNN also developed the major targets of attack of DDoS 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 considered as the significant part for every individual in different ways due to which cyberspace attacks has also been increased. For instance, Information Phishing, Denial of Service, Email Spamming, Financial Fraud, etc. among numerous internet based attacks Denial of Service is considered as very serious and continuous threat in the world of cyber security. Denial-Of-Service is defined as an attack targeted for divesting genuine users with the 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 attacks of DoS are systematized by various dispersed computers, they commonly known as DDoS attack (Distributed Denial of Service). DDoS attack is termed as the of the most widespread attack in the world of cyber and the targets are, Links, Victim's OS Firewalls and defense systems, Routers, Victim's Application, Victim's Infrastructure and Current Communication. Basically different types of attacks of DDoS 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 with every passing day.

Basically two different type of attack of DDoS i.e. typical attack of DDoS and Distributed Reflection Denial of Service attack (shown in figure 2) and both types are cooperated machines which consume to be engaged throughout the process of scanning 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).

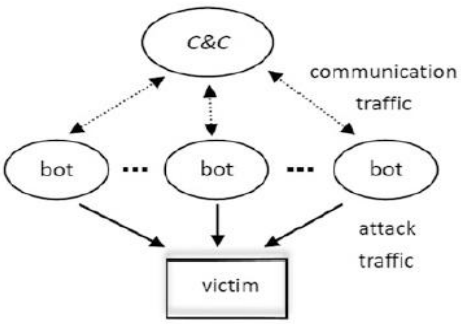

Figure 1: A typical DDoS attack

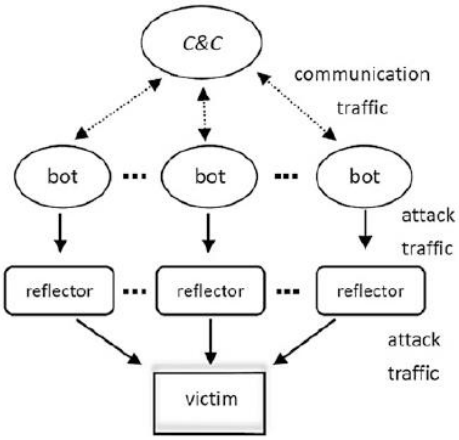

Figure 2: A DRDoS Attack

Causes

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

- In Internet security, high interdependencies exist.
- Inadequate internet resources.
- Several unintentionally compromised hosts, plot against a few target servers of hosts.
- Many a time intelligence and resources are helpful to prevent future attacks and are not frequently collected.
- On internet direct routing principles are used.
- The disparities in speed and design between the edge and primary networks are conventional.
- Loose management of network.
- Basic and beneficial practice of distribution resources has its disadvantages (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 movement helps a DDoS-for-hire service called LizardStresser for launching attack traffic in contradiction of their targets. As the games came closer, LizardStresser with connection of numerous other Internet of Things (IoT) botnets attacked at 540 Gbps. This might include interruption of the media coverage of the Rio Olympics but at the same time with the help of mitigation measures delivered by

Arbor Networks, the the International Olympics Committee (IOC) and Brazilian information security professionals kept their schemes up successively (https://www.tripwire.com).

Review of Literature

Kim *et al.* (2004), discussed about the collective approach of data mining of DDoS attack for the purpose of recognition of the numerous types, which is made by different automatic feature selection module by the help of classifier generation module by neural network and decision tree algorithm.

Elleithy *et al.* (2006), in their paper discussed about the execution and examination of main types of attacks: TCP SYN Flood, Ping of Death, and Distributed DoS. In this paper they demonstrated the possible risk from DoS attacks and examine the consequences of the risk.

Hussain *et al.* (2006), projected and work on the attack fingerprinting system to recognize repeated attack of DDoS. In this paper they concluded that their system is helpful and considered as a new tool that can be helpful to support in prosecution of both criminal and civil which will improve forensic proficiencies of network traffic and later utilizes for the purpose of investigation.

Lu *et al.* (2007), projected a novel structure too robustly and proficiently identify attack of DDoS and also recognize attack packets with an aim to feat temporal and spatial correlation of attack traffic of DDoS. They had design to set anti-DDoS system which is perimeter based where the traffic is examined at the edge routers of an ISP network.

Gupta *et al.* (2008), offered in his work which focused on the recognition of different variety of attacks of DDoS by checking transmission of disturbed traffic changes inside ISP Domain and then personifies flows that convey attack traffic. They undergoes simulation results that, the novel framework can successfully distinguish and characterize different kinds of attack related to DDoS.

Yu and Zhou (2008), focused on the recognition of DDoS attacks in numerous public networks through Entropy-Based Collaborative Detection Method. In which they calculated flow of entropy, they found that in the case of less router entropy as comparison with given threshold, then there is higher attack alarm and on the supposed flow the routers will estimate the amount of entropy of the suspected flow. There is also the condition when the rate of entropy is similar or not similar or less with comparison with the given value, then it is conclusive that attack is done. The present study focused that with the combination of entropy rate of flows and router entropy it is possible to differentiate attack of DDoS from the accessing of surge legitimate and hence examination of attack at early stage is seen.

Kumarasamy (2011), proposed a method which provides the strong defense against DDoS attacks. It very easily recognizes the host of the attacker by dealing with their nature of traffic and hence 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 suggested a new cracking algorithm for the purpose of preventing the attacks of DDoS. 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 indication for the proposal is to defend the server or network from DDoS attacks. This new cracking algorithm successfully provide the accessibility of web services at the time of DDoS attack.

François *et al.* (2012), proposed FireCol to overcome with the problem of DDoS attacks. It is scalable solution for primary recognition of DDoS attacks and composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. FireCol gave good result and focussed good practices for its related 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 stated about the EM algorism for estimating the Gaussian mixture distribution model of circulation parameter and a technique to identify anomalies in network traffic.

Devi and Yogesh (2012), proposed an operational and competent scheme of defense against attacks of DDoS dependent on entropy. This methods basically delivers a twice check point for detection of malicious flow from the normal flow.

Mahajan and Sachdeva (2013), focus mainly on attack of DDoS attack which hampers the network or server availability. They also discussed the different techniques which are used to avoid and moderate these rounds with concerning advantage and disadvantage. Different prevent and mitigation techniques are Route Based Distributed Packet Filtering, Secure Overlay Services (SOS) Ingress Filtering, Load Balancing Egress Filtering, History Based IP-Filtering, 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 provide prevention for oneself from any attack of DDoS.

Zlomislić *et al.* (2017), focused on the current review of denial of service (DoS) attack and its related defense concepts, from both the point of consideration i.e. theoretical and practical and proposed for future research.

Conclusion

According to the review study, it has been concluded the inspite of several preventive of DoS attack, numerous are also different insecure machines over the internet that can promote large-scale of attack of DDoS. 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 attak researchers have to effectively work to progress a complete result that includes several activites of defense for the purpose of trapping of different attack of DDoS.

References:

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.

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

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.

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/.

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.

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

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.

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.

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.

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.

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.

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.

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

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