Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 3, March 2021, pg.83 – 88

Distributed Denial of Service (DDoS) Attacks and Defence Mechanism

Akhil K.M[1]; Rahul C.T[2]; Athira V.B[3]

[1]Student, Dept. of computer Application, SNGIST Arts & Science Collage, MG University, India
[2]Student, Dept. of computer Application, SNGIST Arts & Science Collage, MG University, India
[3]Assistant Professor, Dept. of Computer Applications, SNGIST Arts & Science Collage, MG University, India
akhilmurali500@gmail.com; Rahulct222@gmail.com; studyin32@gmail.com

DOI: 10.47760/ijcsmc.2021.v10i03.010

Abstract— Denial of Service (DoS) attacks is one of the major threats to Internet sites and one of the major security problems Internet faces today. The nature of threats caused by Distributed Denial of Service (DDoS) attacks on networks. With little or no warning, a DDoS attack could easily destroy its victim's communication and network resources in a short period of time. This paper outlines the problem of DDoS attacks and developing a classification of DDoS attacks and DDoS defense mechanisms. Important features of each attack and defense system category are described and advantages and disadvantages of each proposed scheme are outlined. The goal of the paper is to set a certain order of existence methods of attack and defense mechanisms, for the better understanding DDoS attacks can be achieved with more effective methods and means of self-defense can be developed.

Keywords— DoS attacks, DDoS attacks, DDoS Defenses, Network security, Intrusion detection.

I. INTRODUCTION

Denial of Service (DOS) attacks is a major problem Internet faces. Denial-of-service attack (DoS attack) is a cyber-attack within which the perpetrator seeks to make a machine or network resource unavailable to its users with the intention of temporarily or permanently disrupting services of an Internet based administrator. Denial of service is usually achieved by flooding the targeted network or resource with an unnecessary request in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. The main purpose of DOS is to interrupt services by trying to limit access to a machine or service instead of interrupting the service itself. This type of attack is intended to give the network the ability to provide standard services by identifying the network bandwidth or its connection. In a distributed denial-of-service attack (DDoS attack), the incoming traffic floods the victim from a variety of sources. This effectively makes it impossible to stop an attack by simply blocking a single source. DDoS attacks can add a one-to-one magnitude to the DOS problem making blocking more difficult and more effective.

In this paper we are trying to combat these issues by introducing defense mechanism by presenting the DDoS attack problems. Our aim is to clarify the issues that exist in order that a higher understanding of DDoS attacks can be found and better ways and means of self-defense.

Following the introduction, this paper is organized as follows. Section 2 consists of DoS attacks classification and problems. Section 3 consists of DDoS attacks classification and problems. Section 4 consists of DDoS defense mechanisms, while section 5 concludes the paper.

II. DOS ATTACKS

DoS attacks are considered to occur only when access to a computer or network service is intentionally blocked or downgraded due to malicious activity by another user. It can be defined as an attack designed to deny a computer or network the ability to provide standard services. These attacks do not damage data directly or permanently, but endanger the availability of resources. A DOS attacks are considered to occur only if access to a computer or network service is blocked or intentionally reduced due to malicious activity by another user.

DoS attacks are classified on the basis of the attacked protocol level of five categories as follows:

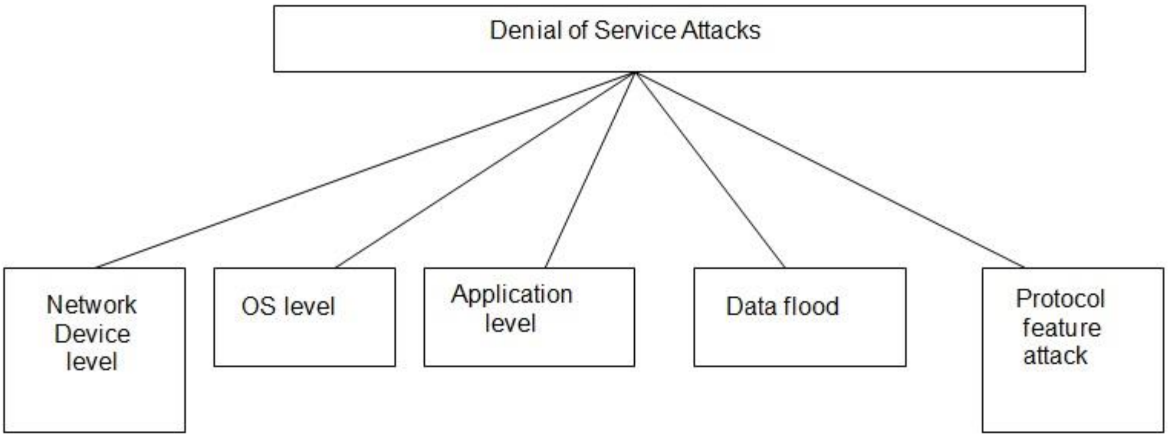

Fig. 1. Classification of Denial-of-Service attacks

Network Device Level: DOS attacks on Network Device Level include attacks that might be caused by bugs in the software or by attempting to destroy hardware devices of network devices.

OS Level: There might be flaws in the operating system implemented protocols, the DoS attacks will take advantage of these flaws to attack the user.

Application-based attacks: An application-based attack targets computer by deliberately causing a mistake in a computer's applications. This allows the attacker gaining the ability to bypass normal access controls. Application-level attacks can be performed on a client computer or server.

Data Flooding: In a flood attack, attackers will try to send massive amount of data to the host by using bandwidth availability of the network. This will overload the server with high amount of traffic, causing the sever non-responsive.

Attacks based on protocol features: DOS may take advantage of certain standard protocol features, for example several attacks exploit the fact that IP source addresses can be spoofed.

III. DDOS ATTACKS

3.1. Definition of DDoS attacks and strategies

DDoS attacks use multiple computers to launch systematic DOS attacks in one or more directions. Using customer / server technology, the perpetrator is able to duplicate DOS performance significantly through the use of many inactive computer accomplices, which act as attack platforms.

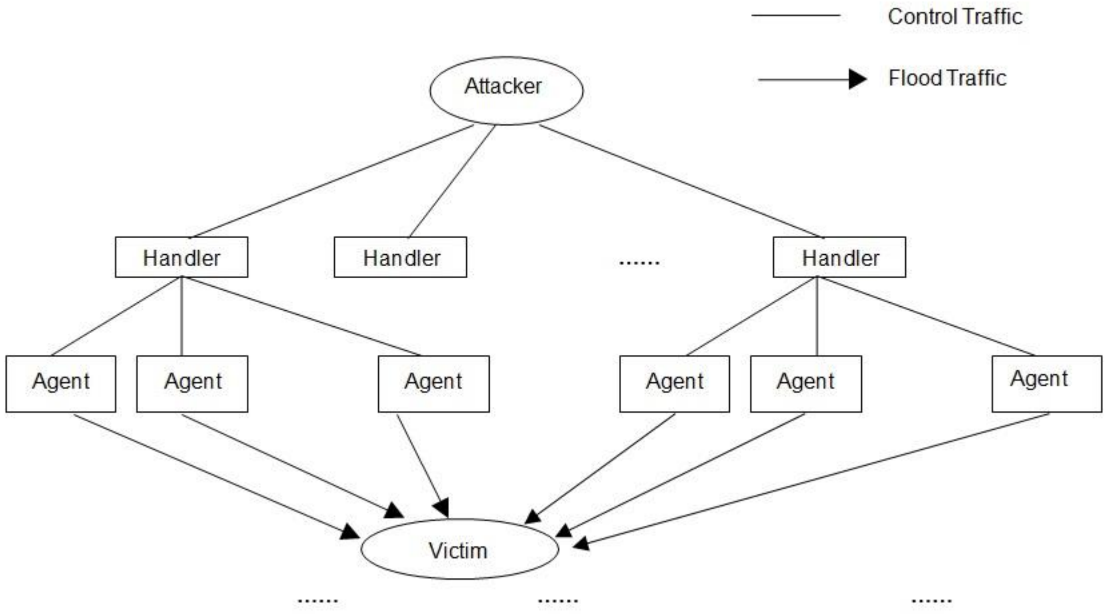

Fig. 2. Architecture of DDoS attacks.

A DDoS attack is composed of four elements, as illustrated in the above figure (Fig.2).

- The Real attacker.
- The Handlers or master compromised hosts, who are capable of controlling multiple agents.
- Daemon agents or zombie hosts, who are responsible for producing packet distribution to the intended recipient.
- A victim or host.

A Distributed Denial of Service Attack can be described as follows:

Recruitment: The attacker selects vulnerable agents, which will be used to carry out the attack.

Compromise: The attacker uses the agent's risk and imports the attack code, protecting it simultaneously from detecting and deactivating.

Communication: The agents notify the attacker using administrators that they are ready.

Attack: The attacker orders the start of the attack.

Sophisticated and powerful DDoS tools are available to attackers which may increase the risk of becoming a victim of DOS or DDoS attack. Some of the most known DDoS tools are Trinoo, TFN(Tribe Flood Network), Stacheldraht, TFN2K, mstream and Shaft.

3.2. DDoS attack classification

Bandwidth depletion and resource depletion attacks are the two main classes of DDoS attacks. Bandwidth end attacks are designed to flood the victim's network with an unwanted traffic that prevents official traffic from accessing the victim's system. Resource reduction attacks are attacks designed to bind the victim's system resources. This type of attack can be divided into protocol exploitation attacks and malicious packet attacks.

IV. CLASSIFICATION OF DDOS DEFENCE MECHANISM

4.1. Intrusion Prevention

The best strategy against DDoS attack is to completely prevent the attack even from happening. We try to prevent the attack from being launched in the first palace. There are certain defence mechanism that helps the systems from attackers.

Globally coordinated filters: Using globally coordinated filters, attacking packets can be stopped before they aggregate to lethal proportions. There are different types of filtering mechanisms available:

Ingress filtering, suggested by Ferguson and Senie, is a way to prevent traffic dropping with an IP address that is not the same as the start of a domain connected to an ingress router. This mechanism will be able to drastically reduce the DoS attack by IP spoofing if all domains use it.

Egress filtering, is an output filter, which makes sure that only IP address space which leaves the network are assigned or allocated IP address spaces. Even though does not help in saving wastage of resources, Egress filters will protect other domains from possible attacks.

Route-based packet filtering, approach by Park and Lee is able to filter a large portion of used IP packets and prevent attack packets from reaching their targets as well as to assist in IP retrieval. What’s worse about this method is that it requires a global knowledge of network topology leading to downhill issues.

Disabling unused services: There might be several network services that might be running but not needed or not being used, in order to prevent any incoming attacks these services should be disabled.

Applying security patches: Updating the systems with latest security patches and the use of latest available techniques can reduce the effect of DDoS attacks to a great extent.

Changing IP address: It is one of the simplest and effective solution against DDoS attacks. The method called moving target defence, which is by changing the IP address of victim’s computer, the edge routers will drop the attacking packets when the IP address is changed.

Disabling IP Broadcasts: In an ICMP and Smurf attacks, by disabling the IP broadcasts will no longer act as an amplifier. But in order for this to be effective all the neighbouring network IP broadcasts should be disabled.

Load balancing: IT is an easy way for network providers to increase the bandwidth provided for critical communications and prevent them from crashing in the event of an attack.

Honeypots: Honeypots are programs that are limited in security and can be used to trick the attacker into attacking the honeypot and not the actual systems.

Prevention measures offer increased security but will never completely eliminate the threat of DDoS attacks because they remain vulnerable to new attacks.

4.2. Intrusion Detection

By recognizing anomalies in system behaviours or by using the database of known signatures an Intrusion detection system can detect DDoS attacks. A computer or a network host can protect themselves against DDoS attacks by performing intrusion detection.

Anomaly Detection: Anomaly detection dependent on the discovery of an unusual character with respect to a certain standard. Many anomaly detection systems and approaches have been developed to detect the faint signs of DDoS attacks.

A scalable network monitoring system called NOMAD is able to detect network anomalies by making statistical analysis of IP packet header information. Lee and Stolfo use data mining techniques to find program patterns that describe system performance and user behaviour and calculate a separator that can detect malfunctions and disruptions.

Cabrera et al. propose a Network management System to detect DDoS attacks where selective variables are important for statistical analysis, to achieve the first detection of these attacks.

Huang et al. proposed a mechanism called congestion triggered packet sampling and filtering. In this way, a set of discarded packets is selected due to overcrowding of statistical analysis. When the anomaly is indicated by mathematical results, a signal is sent to the router to filter out malicious packets.

Gil et al. [7] suggested a data formation, which sets back when the discovery of IP addresses participating in DDoS attacks is possible, and measures are taken to block only these specific addresses. This method cannot prevent equal attacks and cannot detect DDoS attacks using multiple Zombies.

Misuse Detection: Misuse detection helps in identifying previous patterns of known exploits and then look at the emergence of such patterns. Many popular network monitors make signature-based acquisitions, such as CISCO'S NetRanger, NID, Realsecure, Snort.

4.3. Intrusion Response

Once the attack is detected, the immediate response is to identify the source of the attack and block its traffic accordingly. There are many ways to track and identify the real source of an attack.

IP traceback: It traces the attack back to its original location, so one can find who the attacker really is and, at the same time, get the appearance of the path. The factors that make the IP traceback difficult are the countless status of the internet routing and the lack of source accountability in the TCP/IP protocol.

ICMP traceback: According to the mechanism proposed by Bellovin that an ICMP traceback message is sent to the destination which every router samples the forwarding packets with a low probability. The source of traffic can be found by forming a chain of traceback messages if enough traceback messages are gathered by the victim. In order to face DDoS attacks by reflectors, Barros [9] proposes a modification of ICMP traceback messages. In this way, routers send ICMP messages to the source of the currently processed package rather than to their destination.

Link -testing traceback: The technique proposed by Burch and Cheswick. It infers the attack path by flooding the links with large burst of traffic and examines whether this induces any perturbation on that network. If so, this link is probably part of the attack method.

CenterTrack: It is an architecture proposed by Stone, which creates an overlay network of IP tunnels by linking all edge routers to central tracking routers, and all suspicious traffic is rerouted from edge routers to the tracking routers.

Probabilistic Packet Marking: It was originally introduced by Savage et al [I2] who described efficient ways to encode partial route path information and include the traceback data in IP packets. Song and Perrig improved PPM performance and suggested the use of hash chain-linking routers. This tagging system works well and is accurate in the face of a large number of DDoS attacks.

Hash based IP traceback: This technique which is introduced by Snoeren et al uses a Source Path Isolation Engine (SPIE) which generates audit trails of trailic and can trace origin of single IP packet delivered by a network in recent past.

V. CONCLUSION

Undoubtedly, DDoS attacks are a serious problem for which numerous defence mechanisms have been proposed. In this paper, we have tried to introduce a method that will allow the separation of the DDoS attack problem so that we can find better solutions. As, this clear view of the problem, our thinking is clarified and in this way we can find better solutions to the problem of DDoS attacks.

Another major benefit of developing DDoS attacks and security divisions is that effective communication and cooperation between investigators can be achieved to detect additional vulnerabilities of the DDoS field. Their number in conducting further research and interviews is undoubtedly high. The next step in this approach would be to create data sets and a test bed so that all these different processes can be compared to the test.

REFERENCES

[1]. P. Ferguson and D. Senie, “RFC 2827: Network Ingress Filtering: Defeating Denial of Service attacks which employ IP source Address Spoofing”, May 2000.

[2]. K. Park and H. Lee, “On the effectiveness of probabilistic packet making for IP traceback under Denial of Service attack”, hoc. IEEE WOCOMM Anchorage, AK, USA, pp. 338-347, Apr. 200I.

[3]. R. R. Talpade, G. Kim and S. Khurana, ‘NOMAD: Traffic-based Network Monitoring Framework for Anomaly Detection”. Proc. 4‘h IEEE Symposium on Computers and Communications, Ted Sea, Egypt, pp. 442451, June 1999.

[4]. W. Lee and S. J. Stolfo, "'Data mining approaches for intrusion detection", 7th USENIX Security Symposium, San Antonio, TX, pp. 79- 93, January 1998.

[5]. J. B. D. Cabrera et al., "Proactive Detection of Distributed Denial of Service Attacks using MIB Traffic Variables - A Feasibility Study", Proc. 7" IFIP/IEEE Int. Symp. On Integrated Network Management, Seattle, WA, May 2001.

[6]. Y. Huang, J. M Pullen, "Countering Denial-of-Service attacks Using Congestion Triggered Packet Sampling and Filtering", Proc. IOth ICCCN, Arizona, USA, Oct. 2001.

[7]. T.M. Gil and M Poleto, "MULTOPS: a data-structure for bandwidth attack detection", Proc. 10th USENIX Security Symposium Washington, DC, pp.23-38, Aug. 2001.

[8]. S. M. Bellavin, "ICMP traceback messages", Internet Draft, 2001

[9]. C. Barros, "A proposal for ICMP traceback messages", Internet Draft, Sept. 2000.

[10]. H. Burch and H. Cheswick, "Tracing anonymous packets to their approximate source", Proc. USENIX LISA, New Orleans, pp.319-327, Dec. 2000.