COMPARATIVE ANALYSIS OF VARIOUS DENIALS OF SERVICE (DoS) ATTACK MITIGATION TECHNIQUES

ADETOYE ADEYEMO

Department of Computer Science and Information Technology,
Bowen University, Iwo, Osun State, Nigeria.
akinyoye2001@yahoo.co.uk

Abstract - The Denial of service (DoS) attack is one of the most widespread attacks that can be used to effectively bring the operation of a host/server to a standstill. One of the motives behind the DoS attack is to make the host/server unreachable to legitimate users. DoS could take one of three possible forms. First, an attacker could stop the network from transmitting the required messages to genuine users on the network. Alternatively, the network could be prompted to generate and spread messages which should not be spreading. The last and the most common form of DoS attack in recent times is an act of generating and transmitting excessive and unnecessary traffic (flooding the network) directed towards a selected network or host/server so as to stop legitimate users from gaining access or receiving the required service from the host/server. Therefore, it is essential to become aware of and mitigate or otherwise minimize the damages and losses that result from the impact of DoS attacks. The main aim of this paper is to critically examine, analyze and compare different DoS mitigation techniques (Mitigation using Hop-Count Filtering, Ingress Filtering, TCP probing for Reply Argument Packet Technique, History-based Attack Detection and Reaction (HADR), Hardware, Extended Access control list, Capability-based method), point out there weaknesses and strengths in order for network administrators to know which mitigation technique(s) will work best for his/her network.

Keywords: Denial of Service, Hop Count Filtering, Ingress Filtering, TCP probing for Reply Argument Packet Technique, History-based Attack Detection and Reaction (HADR), Extended Access control list, DoS mitigation mechanisms.

I. INTRODUCTION

The DoS (Denial of service) attack is one of the most prevailing attacks that can be used to successfully bring the operation of a host or server to a halt. Through this act, the host or server will not be reachable or will not be able to accommodate legitimate users requests. DoS attack is used to flood a network with an excess number of request that a server might not be able to hold, leading to service disruption.

Most of the DoS mitigation techniques used today focus on mitigating the effect of an on-going attack or an attack that had already taken place. Ciza et al, [1] in their paper further classify all of these countermeasure techniques into network-based and client-based, both of which have been employed in different cases. Some of the DoS mitigation techniques that will be examined in this study are Hop-Count Filtering, Ingress Filtering, TCP probing for Reply Argument Packet Technique, History-based Attack Detection and Reaction (HADR), Extended Access control list, Rate limit and Rate limit using Iptable. Various network based mitigation techniques applies definite policies that separate some parts of the network from others and can minimize the effect of an attack on the network. Several methods offer defense by adjusting the physical or logical configuration of the network or its servers [1].

Server-side countermeasure technique protects a server from a DoS attack by making some particular changes to the server. Yang Xiang [2] in one of his papers was of the opinion that a DoS aware algorithm permits the operating system to alleviate the DoS attack by regularly scanning the TCP connection queue and drop half-open connections. This helps to prevent the TCP SYN flood attacks.

II. REVIEWED WORKS

A. MITIGATION USING HOP COUNT FILTERING.

This is a mitigation method that is deployed on destination network equipment (Routers), which is used to deny or drop malicious traffic with a spoofed address [3]. In a given network, the IP address of each host and the corresponding distance to each router are noted and kept in a database. Whenever a packet gets to the router, the router matches the source IP address and the corresponding distance with that in the database. If the distance traveled by the spoofed packet is different from that traveled by a packet originated from the real spoofed source, consequently, the packet is categorized as an attack then it is been drooped. However, the drawback of this method is that the database must be updated with the source addresses and the corresponding distances. This might prove difficult due to route changes [4].

B. MITIGATION USING INGRESS FILTERING.

Ingress filtering is one of the simplest forms of DoS mitigation techniques [5, 6]. This method can be used to stop an attack or malicious traffic with a spoofed IP addresses. The edge router is configured to deny or drop packets that have the source address as one of the IP addresses of the internal network [7]. This means that packets with a spoofed IP address will be denied access into the network. However, for network ingress filtering to be operational and effective, it must be implemented on all entry point into a given network. David et al, [8] in their paper faulted this method because of the administrative overhead it tends to impose for initial deployment and maintenance [8]. However, this should not be an issue as long as it is combined with other mitigation techniques.

C. MITIGATION USING TCP PROBING FOR REPLY ARGUMENT PACKET TECHNIQUE.

Mitigation using TCP probing for Reply Argument Packet Technique is proposed in [9]. TCP SYN flood attacks are one of the most noticeable attacks that consume the network bandwidth. The SYN flood attack exploits the weakness of the TCP three-way handshakes. A server needs to apportion a large data structure for any SYN packet that is trying to initiate a connection to the server notwithstanding the authenticity of the packet. What the network is concerned with is the reachability of the destination, while the attacker tries to spoof the source IP address as an honest source of the server. This is called IP spoofing. Throughout the three-way handshake when the server logged the request information into the memory stack, the server will have to wait for validation from the client that sends the request. The server will not receive confirmation packets for the request created by SYN flood attack as the IP addresses used in SYN flood attacks may be a fake IP address. Such half-open connections will remain in the memory until it timed out. The server retransmits the SYNACK five times, doubling the time out value after each retransmission. Hence no new requests including legitimate requests can be processed and the services are disabled [9].

In order to mitigate TCP SYN flooding Felix Lau et al, [10] suggested a scheme which is called TCP probing for Reply Argument Packet method. This mitigation technique is configured on a server, it can be used to distinguish between spoofed and legitimate IP address and at the same time, it can be used as a countermeasure for DoS attacks. This method logically attaches TCP acknowledgment to give an added layer of protection. According to Felix Lau et al [10], the receiver host/server sends acknowledgment that should change the TCP window size or cause packet retransmission. In a situation where the source machine does not retransmit the packet, the server then concludes that the packet's source is being spoofed. The drawback of this method is that, when a legitimate host sends a SYN request to a server and the server was able to send back a cause packet retransmission to the host and while the host is trying to retransmit there is a network failure, then the server drops the previous SYN request concluding that the IP address is spoofed. So this mitigation technique is not going to be productive in a situation where there is frequent network failure.

D. MITIGATION USING HISTORY-BASED ATTACK DETECTION AND REACTION (HADR).

This mitigation technique was proposed by Toa [11] with collaborations from other authors [12]. This mitigation technique was classified as one of the simplest forms of DoS attack countermeasures in the sense that, it does not require any form of programming or technical knowledge. All that is needed is the collection of IP addresses; this is done based on the network connection history to the victim/server. All IP addresses that are classified as legitimate users that have in the previous time accessed the victim are collected and stored in the memory/database of the victim. Whenever a connection request is sent to the victim, it compares the source IP address against the IP address database, if the source IP address is found in the database, then the connection is permitted, but if the Source IP address is not in the database, the connection is dropped.

The drawback of this countermeasure technique is that;

- Rigour of inserting a new IP address into the database. Whenever a new host or machine is added to the network, the network administrators have to include the machine's IP address into the database.
- This method is prone to address spoofing. It is possible that an attacker gets hold of the addresses in the database and used it as a source of a packet destined to the server.
- While compiling an IP address database, there is a possibility of omitting a legitimate IP address, this implies that the omitted IP address will be automatically blocked by the server.
- A legitimate user that is accessing the server for the first time and host that have their IP address changed will also be blocked.
- Lastly, this method does not protect an attacker from gaining access to the entire network (other hosts on the network).

History based packet filtering system is ineffective when the attacks come from legitimate IP addresses. It also involves an offline database to keep track of IP addresses. Therefore, a high cost is incurred in the information storing and sharing [13].

E. MITIGATION USING HARDWARE

Apart from using software and configurations for DoS mitigation, hardware can also be used. S. Kumar and R. S. Gade [14] in their paper evaluated the effectiveness of a security device called Netscreen 5GT; a product from Juniper. This device Netscreen has a built-in TCP-SYN proxy protection and UDP protection features to guard the network against TCP-SYN flood DoS attacks and UDP flood attacks respectively. The effectiveness of this security device was tested under the Layer-4 flood attack at diverse attack loads.

Kumar and R. S. Gade carried out a real experiment to measure the degree of the effectiveness of this security device; Netscreen 5GT when TCP SYN and UDP flood attacks are being carried out. It was found that the Netscreen 5GT effectively mitigated the impact of DoS attack to some degree particularly when the attack is of lower intensity. However, the device was unable to provide any protection against Layer 4 flood attacks when the traffic intensity was about 40Mbps and above [15]. This method will be effective in a home, office or small network where the rate of transmission or bandwidth usage is not more than 40Mbps.

F. MITIGATION OF ATTACK USING EXTENDED ACCESS CONTROL LIST

Access control lists are sets of rules that permits or denies traffic through a device or into a network. Access lists are basically list of deny and permit statements that are applied on a router or switch interfaces to screen malicious traffic. In order to mitigate the DoS attack, we need to detect and classify the attack in types in order to explicitly write and include the ACL rule that will drop or permit traffic into the list ACL rules. To detect and classify attack traffic we add various ACLs matching to different types of traffic ICMP, TCP, UDP, etc on router or switch interfaces [15]. ACLs have got a facility that counts the number of packets, size ACL match, source and destination address that flows through the interface where the ACL is applied. Malicious and legitimate traffic can easily be categorized by periodically accessing the counter. Whenever malicious traffic is detected from the counter, an ACL rule is set to deny such traffic next time it tries to gain access into the network. Consequently, the rule set will deny all malicious traffic access. However, whenever there is a long list of ACL rules and packet flood, ACL consumes the CPU power, thereby depriving the router of its primary function which is routing. Also, classifying compound DoS attacks with ACLs where the attack traffic might differ with time would be a bad idea, as ACLs needs human intervention [6].

G. MITIGATION OF ATTACK USING CAPABILITY BASED METHOD

Capability-based mechanisms were developed to control the flow of traffic directed at the destination machine. In this mechanism, the machine that wants to initiate a connection or send a message first sends a request for connection packet to the destination. As the packet travels through the network, each router along the path appends a router mark (precapability) to the request packet. The destination machine checks the packet and decides whether to grant permission or not. If the destination machine replies the source machine with a packet that contains capabilities, then permission is granted, if not, then permission is not granted. As earlier said, capability-based mechanisms were developed to control the flow of traffic directed towards at the destination machine according to its own capability, thereby decreasing the likelihoods of being overwhelmed with unwanted traffic, as packets without capabilities are treated as legacy and might get dropped at the router when congestion happens [16].

Manoj Misra et al [13] in their paper pointed out the limitation of this method, though capability base mitigation provides protection for established network flows, however, it is capable of generating a new type of attack called Denial of Capability (DOC), which prevents new capability-setup packets from getting to their destination. In addition, these systems have high computational power and space requirements.

H. MITIGATION OF ATTACK USING RATE LIMIT

One of the best and easiest ways to stop any form of traffic from consuming the entire link is the rate limit. Rate-limiting is a method used to mitigate the DoS attack, it is a method for reducing the impact of unwanted network traffic on the trusted network and make sure it does not affect the legitimate traffic. For instance, if someone is generating large Web traffic from a Web site, such action could prevent essential traffic from getting to the server, and this could possibly render the servers inaccessible to other legitimate users in the network.

One of the characteristics of the Access Control list is that it sets a form of the boundary between the server’s network and the attacker network completely by blocking all traffic from the attacker’s network to the server. Instead of blocking traffic, rate-limit rather set a limit on the size of the packet and the rate of transmission from the attacker to the server. This technique is implemented by most of the Internet service providers as it demonstrates to be very effective and prevents the network from been overwhelmed with unwanted traffics. This mitigation technique does not proffer a better solution because it allows the attacker to access the server but with limited privilege. The better side is that the network administrator is capable of limiting the number of traffic that is directed into the trusted network. The rate limit on the data plane is an important mitigation tool. Rate limiting can turn out to be very vital when all traffic to a site cannot be blocked [17].

However, after the configuration and the application of the rate limit on the router interface, it was discovered that all traffics entering the interface are being policed. This means that both the legitimate user and the attacker traffic are limited to the specified rate stated in the rate-limit configuration. Both attacker and legitimate users are accessing the server at the same rate and this should not be. A more convenient and suitable configuration is to include an access-group keyword in the rate-limit command and combine it with an access list that specifies the traffic we want to rate-limit.

Rate limiting will serve its intended purpose of reducing DoS attacks when it is configured on the Internet service provider’s router that connects to the trusted network. This means that when a network is experiencing a flood attack that is consuming the Internet bandwidth, configuring rate limiting on the edge router will not solve the attack problem. Instead, working with the ISP to put rate limiting in place on the ISP's router will lessen the attack.

I. MITIGATION OF ATTACK USING RATE LIMITING USING IPTABLES

The Iptable firewall has a number of useful extension modules that can be used in addition to the elementary firewall purpose. One of such remarkable extensions is the module which permits you to match recent connection, and perform simple regulation on incoming connections [18]. Rate limiting using Iptable is one of the simplest DoS mitigation techniques that are used to prevent the network from been flooded. What it does is that it allows the server to accept a limited number of simultaneous connections, then drop or delay the rest of connections based on the rule set in the Iptable. It can be used to thwart both network and application layer DoS attacks. It also prevents the server from being loaded by accepting more connections than its available resources. Because when a server is loaded with too many connections, new connections will no longer be recognized and this leads to DoS.

Rate limiting can be implemented on the server we are protecting against DoS attack or on the gateways (Router) as discussed in the previous section. In order to strengthen the security of the network, both implementations can be of greater advantage [19]. However, often times it is better to implement rate limiting on the ISP network, doing this will prevent unwanted traffic from getting into or saturating the network.

There are some inherent issues with rate limiting using Iptable and these are:

- It only protects the server on which it is implemented; this means that all other systems are prone to DoS attack.
- If the Iptable rate limit is only implemented in a network as a line of defense, then an attacker already has access to the network and the server itself.
- The administrator needs to differentiate between legitimate and illegitimate traffic in order to be able to assign a number of connection threshold. Because a legitimate user needs to have full access to the server.

III. Figures and Tables

The table below summarizes the mitigation techniques discussed above.

Table 1: Summarizes the advantages and disadvantages of different mitigation techniques.

Mitigation Technique	Advantages	Limitations
Hop count filtering	• Mitigate spoofing.	• Compiling and updating database is tedious. • It Can be affected by route changes.
Ingress filtering	• Simple to configure. • Mitigate IP spoofing.	• Configure and maintenance becomes tedious where there are multiple entries into the network.
TCP probing for Reply Argument Packet	• Authenticates connections. • Does not consume memory usage.	• Not effective where there is frequent network failure.
History-based Attack Detection and Reaction	• Simple to use.	• Prone to spoofing. • It Does not protect the attacker from gaining access to the network.
Hardware (Netscreen 5GT)	• Fewer configurations.	• Not good for traffic above 40Mbps.
Extended Access control list	• Keeps a record of packets that passes through the interface where it is deployed.	• A Long list of ACL rule could consume the CPU processing power. • Prone to error.
Capability-based method	• Mitigate flooding or overwhelming a host with malicious traffic. • Control traffic flow. • Authenticates request before a reply is issued.	• Systems have high computational power and space requirements.
Rate limit	• Prevents the network from been overwhelmed with unwanted traffics.	• It allows the attacker's network to access the server but with limited privilege.
Rate limiting using Iptable	• Simple to configure and use • Used to prevent both network and application layer DoS attacks	• Only protects the server on which it is implemented, other hosts are prone to DoS attack

IV. Conclusion

From the previous section, we have discussed different mitigation techniques and their inherent advantages and disadvantages. We can see that there is no silver bullet way out of the DoS attack. Mitigating DoS attack necessitates a combination of different mitigation techniques. All that network administrator needs to do is to know what the organization goals are as far as providing services to customers and security issues are concern. The organizational goal in providing services to customers is 100% availability, while security goal is confidentiality, integrity, and availability. To attain all these goals and to reinforce the security of a network, different mitigation techniques must be deployed on the network and all these must be done with high availability, minimum computation overhead, minimum networking overhead, and minimum implementation and management time and cost.

In general, for a simple level of attack traffic, a network administrator may want to mitigate this by his/her self. Deploying firewall rules, router Access control lists, rate limiting at the network edge and probably altering the network topology to circumvent the attack are the effortless solution he/she will most likely use to lessen the effect of the attack. These mitigation methods do not guarantee that the network performance will be completely restored to the pre-attack state. However, it will keep the attacker at bay and by doing so legitimate users will be given enough access to necessary servers and services.

REFERENCES

[1] Ciza Thomas, Rejimol Robinson R. R. “Evaluation of Mitigation Methods for Distributed Denial of Service Attacks,” IEEE Conference on Industrial Electronics and Applications (ICIEA), 2012.

[2] Yang Xiang, Ke Li, and Wanlei Zhou, “Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics IEEE Transactions on Information Forensics and Security, vol. 6, no.”,2, pp. 426-437, 2011.

[3] C. Jin, H. Wang, and Kang G. Shin, “Hop-Count Filtering: An Effective Defence against Spoofed DDoS Traffic," Lecture delivered in Proc. ACM Conference on Computer and Communications Security (CCS)' 2003, Washington, DC, October 2003

[4] A Basheer and G. Manimaran, “Victim-Assisted Mitigation Technique for TCPBased Reflector DDoS Attacks,” Department of Electrical and Computer Engineering Iowa State University, USA, URL: http://vulcan.ee.iastate.edu/~gmani/personal/papers/confs/Networking05.pdf

[5] P. Ferguson and D. Senie, “Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing.” RFC 2267, January 1998.

[6] P. Ferguson and D. Senie, \Network ingress filtering: Defeating denial-of-service attacks which employ IP source address spoofing," RFC 2827, May 2000.

[7] F. Baker, “Ingress Filtering for Multihomed Networks.” BCP 84, March 2004.

[8] David A. Wheeler, Gregory N. Larsen, “Techniques for Cyber Attack Attribution.” Institute for Defense Analyses, Alexandria, Virginia, USA. October 2003.

[9] L.Kavisankar, C.Chellappan, A Mitigation model for TCP SYN flooding with IP Spoofing, IEEE-International Conference on Recent Trends in Information Technology, ICRTIT,2011.

[10] F. Lau, S. H. Rubin, M. H. Smith and L. Trajkovic, “Distributed Denial of Service Attacks” IEEE International Conference on Systems, Man, and Cybernetics, Nashville, 8-11 October 2000, pp. 2275-2280.

[11] P. Tao, "Defending against Distributed Denial of Service Attacks," Ph.D. thesis, Department of Electrical and Electronic Engineering, University of Melbourne, April 2004.

[12] T. Peng, C. Leckie and R. Kotagiri. “Protection from Distributed Denial of Service Attack Using History-based IP Filtering.” To appear in the IEEE International Conference on Communications (ICC 2003), 11-15 May 2003, Anchorage, Alaska USA.

[13] B. Gupta, R. Joshi, M. Misra. Distributed Denial of Service Prevention Techniques, International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010

[14] S. Kumar, R. S. Gade, “Experimental Evaluation of Juniper Network’s Netscreen5GT Security Device against Layer4 Flood Attacks”, Journal of Information Security, Volume 2, pp.50-58, 2011.

[15] Vivek Ramachandran, Bleeding Edge DDoS Mitigation Techniques for ISPs, Cisco Systems, Inc. Bangalore, India, 2012.

[16] T. Anderson, T. Roscoe, D. Wetherall, “Preventing Internet Denial-of-Service with Capabilities,” In ACM SIGCOMM Computer Communication Review, Volume 34, issue 1, January 2004, pp. 39-44.

[17] Michael Glenn. "A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment," SANS Institute, August 21, 2003.

[18] Steve, Using iptables to rate-limit incoming connections, Jul 2005, URL: http://www.debian-administration.org/articles/187.

[19] Adetoye Adeyemo, “Denial of Service Detection and Mitigation.” M. Sc. Thesis, Department of Computer Science and Electronics Engineering, University of Essex, Colchester, United Kingdom. August, 2013