REVIEW ON DISTRIBUTED DENIAL OF SERVICE ATTACKS AND THEIR DEFENSE

Madhavi Dhingra

Amity University Madhya Pradesh, Gwalior

ABSTRACT

Distributed Denial of Service attack (DDoS) attack has affected a large number of networks all over the world. It is not a single kinkd of attack; instead it comprises variety of attacks which occur at protocol level as well as application level. These attacks are reviewed in this paper. With attacks, defense comes naturally. Defense approaches regarding DDOS employ several methods and architectures, which are studied in this paper.

Keywords- DDoS Review, DDoS Attacks, DDoS Defense

I. INTRODUCTİON

Denial of Service (DoS) attack is the most popular and emerging threat for the past few years in the world of internet. A denial-of-service attack (DoS attack) denies the intended user to make use of the required resource by making it unavailable. The major goals of attackers are high profile web servers. With the increasing use of internet on every device, these attacks are spreading on a very large scale in numerous forms by many methods. Rather than relying on a single server, attackers could now take advantage of some hundred, thousand, even tens of thousands or more victim machines to launch the distributed version of the DoS attack. A distributed denial of service attack (DDoS attack) is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet [1].

The first well-publicized DDoS attack in the public domain was in February 2000. On February 7, Yahoo was the victim of a DDoS during which its Internet portal was inaccessible for three hours. Analysts estimated that during the three hours Yahoo was down, it suffered a loss of e-commerce and advertising revenue that amounted to about $500,000.

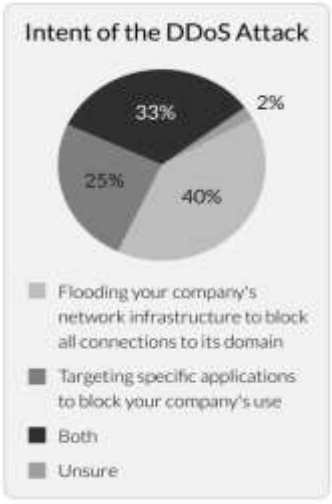

Fig.1 Intent of the DDoS Attack [2]

The impact of this attack was pervasive scale, and therefore network devices and servers are now making greater plans to secure and prevent them from such attacks. According to a survey conducted by incapsula, the intent of DDos attacks were flooding networks infrastructure to block all connections to organization's domain.[2]

II. DDOS ATTACKS

DDoS attacks can be broadly divided into three types:-

2.1 Volume Based Attacks

The attacks make use of large volumes of spoofed packets to flood the network and so as to consume the network bandwidth. Therefore its magnitude is measured in bits per second. It includes UDP floods, ICMP floods, and other spoofed-packet floods.

UDP Flood - This DDoS attack leverages the User Datagram Protocol (UDP), a session less networking protocol. This type of attack floods random ports on a remote host with numerous UDP packets, causing the host to repeatedly check for the application listening at that port, and (when no application is found) reply with an ICMP Destination Unreachable packet. This process saps host resources, and can ultimately lead to inaccessibility.

ICMP (Ping) Flood - Similar in principle to the UDP flood attack, an ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP Echo Reply packets, which results in a significant overall system slowdown.

2.2 Protocol Attacks

Protocol attacks invade at the protocol level. They include SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. Its main goal is to exhaust actual resources such as firewalls and load balancers. The magnitude of Protocol attacks is measured in terms of packets per second.

SYN Flood - A SYN flood DDoS attack exploits a known weakness in the TCP connection sequence (the "three-way handshake"), wherein a SYN request to initiate a TCP connection with a host must be answered by a SYN-ACK response from that host, and then confirmed by an ACK response from the requester. In a SYN flood scenario, the requester sends multiple SYN requests, but either does not respond to the host's SYN-ACK response, or sends the SYN requests from a spoofed IP address. Either way, the host system continues to wait for acknowledgement for each of the requests, binding resources until no new connections can be made, and ultimately resulting in denial of service.

Ping of Death - A ping of death ("POD") attack involves the attacker sending multiple malformed or malicious pings to a computer. The maximum packet length of an IP packet (including header) is 65,535 bytes. However, the Data Link Layer usually poses limits to the maximum frame size - for example 1500 bytes over an Ethernet network. In this case, a large IP packet is split across multiple IP packets (known as fragments), and the recipient host reassembles the IP fragments into the complete packet. In a Ping of Death scenario, following malicious manipulation of fragment content, the recipient ends up with an IP packet which is larger than 65,535

bytes when reassembled. This can overflow memory buffers allocated for the packet, causing denial of service for legitimate packets.

2.3 Application Layer Attacks

Application layer attacks target the web servers with the intent to crash them. They target Windows, Apache or other software's. These include Slowloris, Zero-day DDoS attacks. It is measured in requests per second.

Slowloris - Slowloris is a highly-targeted attack, enabling one web server to take down another server, without affecting other services or ports on the target network. Slowloris does this by holding as many connections to the target web server open for as long as possible. It accomplishes this by creating connections to the target server, but sending only a partial request. Slowloris constantly sends more HTTP headers, but never completes a request. The targeted server keeps each of these false connections open. This eventually overflows the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients.

HTTP Flood - In HTTP flood DDoS attack, the attacker exploits seemingly legitimate HTTP GET or POST requests to attack a web server or application. HTTP floods do not use malformed packets, spoofing or reflection techniques, and require less bandwidth than other attacks to bring down the targeted site or server. The attack is most effective when it forces the server or application to allocate the maximum resources possible in response to each single request.

Zero-day DDoS Attacks - "Zero-day" is simply unknown or new attacks, exploiting vulnerabilities for which no patch has yet been released. The term is well-known amongst the members of the hacker community, where the practice of trading Zero-day vulnerabilities has become a popular activity.

III. DDOS DEFENSE

The implementation of defense system is done either on an autonomous system or distributed system. Autonomous system uses a single node for detection of an attack and responding to an attack. While a distributed defense uses number of systems interconnected over the network which can be implemented anywhere on the network.

Defense regarding DDoS are performed in terms of prevention and detection and response.

Thus DDoS defense mechanisms are categorized into following three types [1] –

3.1 Survival Mechanisms

The goal of survival mechanisms is to limit the effect of DDoS attacks by inclusion of increased resources. Special load balancing techniques are used to maintain and increase the system capacity and performance. But it's not a foolproof approach as attackers can make thousands of zombies to attack multiple resources.

3.2 Proactive Techniques

These techniques aim to detect the attack before they occur. Once attack is detected, the attack lessening approach is followed.

3.3 Reactive Mechanisms

Reactive techniques are performed after an attack occurs on the services of the victim. In this technique, a detection and mitigation process is called to determine the source of the attack and filter the traffic from the attack. They respond to attack by controlling the stream of attack or by finding out the location of the zombie

machines and react to that either by controlling attack streams, or by attempting to locate agent machines and invoking human action. There have been numerous proposals and partial solutions available today for react to the DDoS attack. These mechanisms are further classified into spoofing based and non-spoofing based techniques involving ingress filtering, traceback etc.

Attack is detected following patterns or anomalies. In pattern detection, the identification pattern of known attacks is stored in database. Signatures are used as identification. Anomaly detection makes a model of normal system behavior. It compares the current system features with the expected normal system model. Anomaly detection procedure can also detect unknown attacks.

IV. DEFENSE ARCHİTECTURES

There are four primary factors involved in defense.

1. Agent Identification – This is the procedure that determines the attacking machines and provides their information to the victim machines.
2. Rate limiting – These mechanisms set the limit on the stream of data that can be treated as malicious.
3. Filtering - These mechanisms filter out the attack streams based on the characteristics set by the detection mechanism.
4. Reconfiguration – These mechanisms change the configuration of network by changing the topology of the victim machine or add more resources to isolate the attacks.

Depending on the deployment locations, three kinds of defense architectures are in use [4].

4.1 Source-End Defense Mechanisms

A generic architecture of source-end defense schemes is shown in Figure 2. The choking component imposes rate of outgoing connections. The Detection engine is used for comparing each incoming and outgoing traffic statistics based on predefined profiles. It detects as well as stops DDoS attack at the source and thereby prevents the flooding towards the whole network. The limitation of this approach is that it is not capable of detecting stack when sources are distributed in a wide area.

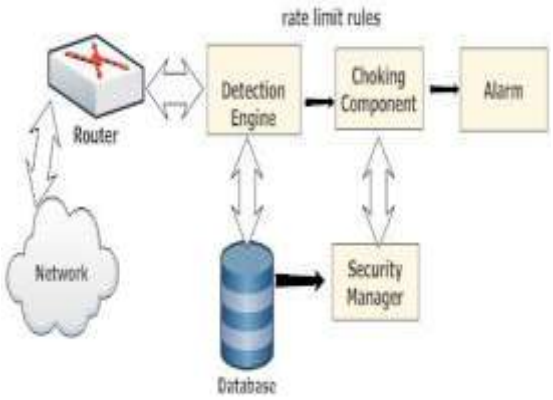

Fig. 2 Architecture for source-end DDoS Mechanism [4]

4.2 Victim-End Defense Mechanisms

This defense is implemented on the routers of victim networks. When resource utilization increases at routers, these routers are designated as victim. Thus it is essential to secure the network resources used by web servers. The only drawback of this approach is that the attack can be detected only after it attacks victim.

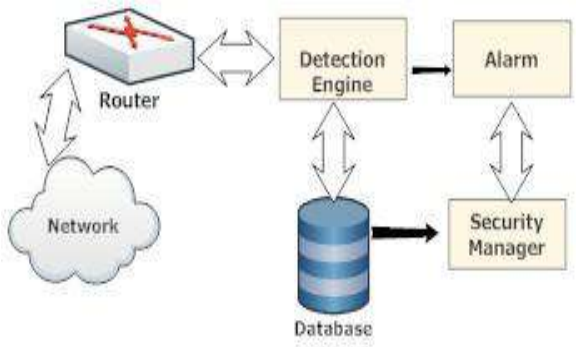

Fig. 3 Architecture for Source-End DDoS Mechanism [4]

4.3 Intermediate Network Defense Mechanisms

The intermediate network defense scheme balances the trade-offs between detection accuracy and attack bandwidth consumption, the main issues in source-end and victim-end detection approaches. Figure 3 shows a generic architecture of the intermediate network defense scheme which can be used in any network router. Such a scheme is usually cooperative in nature and also the routers share their observations with other routers. Like a source-end scheme, these schemes also impose rate limits on connections passing by the router when scrutiny with hold on normal profiles.

In this approach, detection and traceback of attack sources are simple because of cooperative operation. Routers can form an overlay mesh to share their observations. One main drawback of this approach is ability of deployment. All other routers on the network need to employ this detection scheme in order to achieve full detection accuracy. Obviously, full practical implementation of this scheme is extremely tough by reconfiguring all the routers on the Internet.

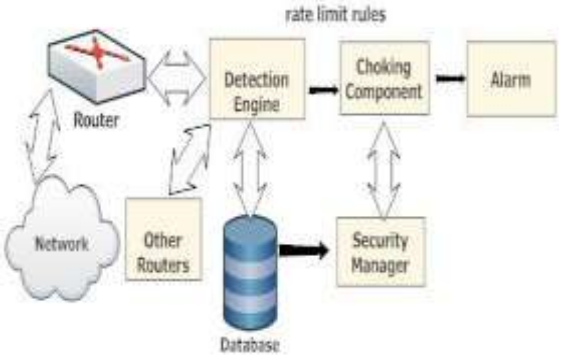

Fig. 4 Architecture for Intermediate Network Based DDoS Mechanism [4]

V. ATTACK DETECTION METHODS REVIEW

The work done on DDoS attack detection mechanism is classified under three basic methods [4].

5.1 Statistical Methods

Statistical properties of normal and attack patterns could be exploited for detection of DDoS attacks. A statistical inference test is applied to see whether any new instance belong to statistical model of normal traffic. Most common DDoS defense scheme is D-WARD [7]. A DWARD system is installed on source router that acts as gateway between the source network and the internet. It identifies an attack based on continuous watching of two way traffic between the two networks. Some other schemes are also proposed based on this method.

5.2 Knowledge based Methods

In this type of method, attack events are checked against predefined patterns of attack. These approaches make use of expert system. Examples of these approaches embody self-organizing maps and state transition analysis.

5.3 Soft Computing Methods

Soft computing comprises processing techniques that bear with imprecision and uncertainty.

Several methods are proposed that detect the network status and guard network servers, routers and client hosts. Zhong and Yue [8] present a DDoS attack detection model which extracts a network traffic model and a network packet protocol status model and sets the limit for the detection model. Captured network traffic values are clustered based on the k-means clustering algorithm to build initial threshold values for network traffic. All captured packets are used to build the packet protocol status model using the Apriori and FCM algorithms [9].

VI. CHALLENGES WITH PRESENT TECHNOLOGY

Many problems exist while implementing defense mechanisms. They are [10]-

(a) Large number of unwitting participants,

(b) No common characteristics of DDoS streams,

(c) Use of legitimate traffic models by attackers,

(d) No administrative domain cooperation,

(e) Automated tools,

(f) Hidden identity of participants,

(g) Persistent security holes on the Internet,

(h) Lack of attack information and

(i) Absence of standardized evaluation and testing approaches.

VII. CONCLUSION

DDoS attacks are increasing by leaps and bounds consequently. Their defense approaches are also refined periodically. After studying number of architectures and methods of defense, it is understood that attacks have their own features and in accordance with that, preventive techniques are used. However, success of defense techniques depends on the nature of attack and its level and implementation of defense method, especially in terms of unknown attack. Several methods and tools exist today for preventing the networks against these attacks. The need for modification occurs when some new kind of attack comes in the network.

REFERENCES

[1] A Survey on Solutions to Distributed Denial of Service Attacks, Shibiao Lin Tzi-cker Chiueh, Department of Computer Science, Stony Brook University, Stony Brook, NY-11794

[2] Incapsula Survey:What DDoS Attacks really Costs Business- DDoS Impact Survey

[3] Survey on DDoS Attacks and its Detection & Defence Approaches, Nisha H. Bhandari, International Journal of Science and Modern Engineering (IJISME), ISSN: 2319-6386, Volume-1, Issue-3, February 2013, pp. 67-71

[4] Dileep Kumar, Dr CV Guru Rao, Dr Manoj Kumar Singh, Dr Satyanarayana, A Survey on Defense Mechanisms countering DDoS Attacks in the Network, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 7, July 2013

[5] Ms. Anuja R. Zade, Dr. Suhas .H. Patil, A Survey On Various Defense Mechanisms Against Application Layer Distributed Denial Of Service Attack, International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397 Vol. 3 No. 11 November 2011, pp.3558-3563

[6] S.Karthik, Dr. V.P. Arunachalam, Dr.T.Ravichandran , An Analysis Of DDoS Attack Methods, Threats, Tools And Defense Mechanisms, IJERIA-An Analysis of DDoS Attack Methods Threats Tools and Defense Mechanisms

[7] Mirkoviac, J., Prier, G., and Reiher, P. (2002) Attacking DDoS at the source. Proceedings of the 10th IEEE International Conference on Network Protocols, Paris, France, 12-15 November, pp. 1092–1648. IEEE CS.

[8] Zhong, R. and Yue, G. (2010) DDoS detection system based on data mining. Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan, China, 2-4 April, pp. 062–065. Academy Publisher.

[9] Agrawal, R. and Srikant, R. (1994) Fast algorithms for mining association rules in large databases. Proceedings of the 20th International Conference on Very Large Data Bases, Santiago de Chile, Chile, 12-15 September, pp. 487–499. Morgan Kaufmann.

[10] B. B. Gupta, Student Member, IEEE, R. C. Joshi, and Manoj Misra, Member, IEEE International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010 pp.1793-8163

[11] Akamai‘s Prolexic Quarterly Global DDoS Attack Report Quarter 1 of 2014

[12] Arbor’s ninth Annual Worldwide Infrastructure Security Report (WISR), released march,2014, mim.umd.edu/wp-content/uploads/2012/10/arbor_networks_issue2-2.pdf