A Review of Distributed Denial of Service Attacks

Sujini Priscilla J[1] Hajiram Beevi J[2]
[1]Research Scholar [2]Assistant Professor
[1]Department of Computer Science [2]Department of Computer Science & Information Technology
[1,2]Jamal Mohamed College (A), Tiruchirappalli 620 020

Abstract— In the current era, Internet plays a vital role in communication which can be used by millions of users across the network. At the same time, the commercial nature of Internet is increasing the vulnerabilities in usage. Distributed Denial of Service Attack (DDOS) is one of the most dangerous threats to the Internet security. Recent studies show that the volume of DDOS attacks reached over 100 Giga bit per second. Furthermore, the volume of DDOS attack traffic has been increasing in size year by year. A DDOS attack is a malicious attempt to prevent legitimated clients from using network resources, usually by temporarily interrupting or suspending the services of a host connected to the Internet. This survey paper deals with the introduction of DDOS attacks, characteristics and elements of DDOS attacks and classification of the various DDOS attacks. Finally, direction for future research work has been pointed out.

Key words: DOS attack, DDOS attack, Cloud Computing, HTTP, XML

I. Introduction

Cloud computing is a long dreamt imagination of computing as a utility. It is a well-known facility to the client known for its pay on claim service. The most important feature of this technique is ease of access and ease of use. As it offers virtualized services and resources to the client via internet. So there is a foremost issue of security in the client side along with in the server side. If security is not reliable and strong, the flexibility and the benefits provided by the cloud computing will lose its credibility. The importance of cloud computing is increasing and it is receiving a growing attention in the security issues.

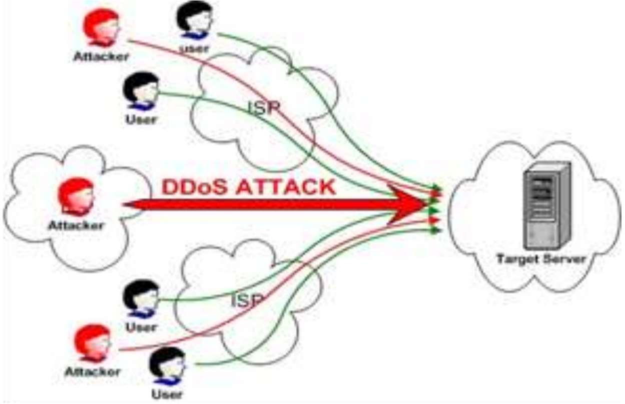

Fig. 1: Fundamentals of DDOS attacks

As moving a huge amount of data into the cloud environment, the attackers are eager to utilize the vulnerabilities associated with it and thereby to steal the sensitive data. Although Cloud Service Provider offers some conventional security mechanisms still there are more non identifiable attacks have been initiated against the cloud environment. One such attack is Denial of Service attack. The main goal of DOS attack is to make the network resources such as Internet, Web services and applications not accessed by the legitimated clients for a certain period of time. DDOS (Distributed Denial of Service) is the superior form of DOS attack. DDOS are a substantial problem because they are very tough to detect, there is no comprehensive solution and it can seal an organization off from the internet [1]. The fundamental of Denial of Service Attack is shown in Fig. 1.

The rest of the paper is organized as follows. The Section II presents the elements and characteristics of DDOS attack. The Section III explains the types of DDOS attacks. The Section IV deals with the specific DDOS attacks associated with Cloud environment. The Section V depicts the Cloud Trace Back mechanism. Finally, conclusion and future direction presents in Section VI.

II. DDOS Attack

A DDOS attack is a malicious attempt to prevent legitimated clients from using network resources, usually by temporarily interrupting or suspending the services of a host connected to the Internet. This section describes the characteristics and elements of DDOS attacks.

A. Characteristics of DDOS Attack

- Routing table in a host or gateway is altered.
- HTTP requests are flooded via port 80.
- Flags in the UDP and TCP protocols are manipulated.
- An IP address of source and destination and port number of packet are accidentally generated.
- For whole attack period, size of packet, sequence number and window size are static [2].

B. Elements of DDOS Attack

1) Victim: Receives the blunt of the attack.
2) Attack Daemon Agents: Agent programs that actually carry out the attack on target victim.
3) Master Program/Agent: Synchronizes the attack through the attack daemons, also known as handler.
4) Attacker/Attacking Hosts: Mastermind behind the attack using the master which stays behind the scenes during the real attack, which makes it difficult to trace. To do all this attacker has to work hard on it he/she need to learn the network topology and its vulnerabilities that can be utilized during the attack [3].

III. Types of DDOS Attacks

A DDOS attack may appear under any of the following classifications.

A. Volume Based Attacks / Bandwidth Based Attacks:

This form of attack involves a huge number of requests being sent to the target system and the system may recognize them to be valid or invalid requests. The valid requests are assumed to be spoofed packets and invalid ones are to be called as malformed packets. The requests can be across a range of ports on your system. This category attacks includes UDP floods, ICMP floods. The main objective of this attack is to saturate the bandwidth of the target system so that the legitimate users could not access it.

B. *Protocol Attacks:*

Protocol based attacks are implemented on load balancers or servers which abuse the way that system converse with each other. The packets can be considered to make the server wait for a non-existent response throughout the normal hand shake protocol. Example: Ping of death, smurf attack, SYN floods, fragmented packet attack etc. The magnitude of this attack is measured in packets per second.

C. *Application Layer Attacks:*

Hackers use branded vulnerabilities in the web server's software or application software crack to root the web server to hang or crash. The greatest common application based attack is to send partial requests to a server to shot to use up (ie make busy), the entire database connection pool of the server which in turn blocks authentic and blameless requests. This type of attack concentrates on specific web application and sends HTTP requests the limit it can handle HTTP DDOS attack and XML DDOS attack or REST based attack.

IV. SPECIFIC DDOS ATTACKS ON CLOUD

To understand the DDOS attacks better, they are analyzed individually in the following section.

A. *SYN Floods:*

TCY SYN flood is a one of the most known and used resource depletion attack. A SYN flood attack occurs during a three-way handshake that a client requests a new connection by sending a SYN packet to the server after which the server sends a SYN/ACK packet back to the client and places the connection request in a queue. Finally, the client acknowledges the SYN/ACK packet. If an attack occurs, then the attacker's sends an abundance of SYN packets toe the victim, obliging it both to open a lot of TCP connections and to respond to them. Then the attacker does not execute the third step of the three-way handshake that follows, rendering the victim unable to accept any new incoming connections. Mostly the attacker sends a spoofed package to victim, what causes that the SYN/ACK package is sent completely to other host, which do not respond as it did not send and SYN packets to the victim [4].

B. *UDP Flood Attack:*

This is the second and foremost popular DDOS attack method after TCP SYN fold. UDP flood attack generally uses IP address spoofing, so that the attacker can stay away from detection. The basic idea in the UDP Flood attacks is to exploit UDP services, which are known to reply to packets. The hacker is armed with a list of broadcast addresses, to which sends spoofed UDP packets. These packets are sent to Random and changing ports of the unsuspected target location. In most of the cases the packets are directed to the echo port 7 (echoes any character it receives in an attempt to test network programs) on the target machines. However, there are attacks in which the malicious user sends packets to the chargen port. The chargen port is a port, which is used for testing purposes and generates a series of characters for each packet it receives. By connecting a host's chargen service to the echo service on the same or another machine, all affected machines can be effectively taken out of service as an excessively high number of packets are going to be produced. In addition, if two or more hosts are so connected, the intervening network can also become congested and deny service to all hosts whose traffic traverses that network.

It is obvious from the previous analysis that the result from a UDP flood attack is the creation of a nonstop flood of useless data passes between two or more systems. The target host returns ICMP port unreachable messages as a response to each spoofed UDP packets and then slows down because becomes more and more busy processing the forged IP addresses. This loop is responsible for the overload of the network and the total exhaust of the available bandwidth. Victims of this massive amount of traffic can be also, except networks, individual system, which can lose connectivity to the Internet and in some cases, crash [5].

C. *ICMP Flood:*

The bandwidth attack that habits ICMP packets. The victim will be flooded with ICMP echo request packets by the attacker and when the victim efforts to reply, the bandwidth application will be maximized eventually ensuing in networking [6].

D. *Ping of Death:*

This attack guides multiple malformed or malicious pings to a computer. The target system will obtain an IP packet larger than the size permitted by the IP protocol. As per the TCP/IP protocol, this packet will be split at the sender side and reconstructed at the receiver end but when the gigantic packet is getting reassembled, the target system resolve crash or its performance will remain [7].

E. *Smurf Attack:*

The smurf attacker refers an ICMP ping message from a spoofed IP address to a broadcast IP address relatively to a particular system. Hence the target system will be stunned with response messages from all the systems in the network and in this manner it will be prevented from responding to an effective request [6] [7].

F. *Mail Bomb Attack:*

In a mail bomb attack, the attacker directs a large amount of e-mails to a target e-mail address to surplus the victim's mailbox or slows down the mail server. The attacker may generate each e-mail with a altered message to permit the junk filters [8].

G. *HTTP DDOS Attack (HDOS):*

The attacker uses the HTTP GET and POST request messages to flood the victim. The HTTP GET request is normally used for "normal links". Including images; such requests are intended to regain a static piece of data, the URL pointing to that piece of data. When you pass in a URL in the URL bar, a GET is also done POST requests used with forms. A POST request includes parameters, which are typically taken from the input fields on the same page. When flooding, the attacker wants to submerge the target server under many requests, so as to saturate its computing resources. The HTTP POST request id more complex as it involves input data from forms which involves more calculation from the server side [9]. On the whole HTTP POST DDOS attack is more active than the GET flood attack.

H. XML based DOS attack (XDOS):

The aim of this attack is to exhaust the resources and network bandwidth of the server hosting a web service while handling SOAP messages. XML based DOS attacks are extremely asymmetric to deliver the attack payload; an attacker needs to spend only a fraction of the processing power or bandwidth that the victim needs to spend to handle the payload. The other ways of launching XDOS attacks are external entity references and entity expansion [10]. XDOS attacks are very easy to implement as there are very less defense mechanisms used in day to day life.

V. Security approaches for DDOS attacks

A. Cloud Trace Back (CTB)

The Cloud Trace Back (CTB) is used to categorize the cause of the DDOS attack and cloud protector helps to discriminate and screen these attack forms in the years to come. CTB is created on Distributed Packet Marking algorithm (DPM) and the Cloud Protector practices back propagation neural network to detached banned message patterns. CTB is placed before the web server to escape direct DDOS attacks [11]. The efficiency of the model hangs on the effectiveness of the neural network and hence data set plays a vibrant role in deciding the performance of CTB.

Properties and Characteristics of CTB:

- Loosely coupled
- Dynamic discovery
- Late binding
- Policy based behavior

B. Cloud Protector

CTB does not directly eliminate a DDoS attack message. This is left for the filter section of a defence system called Cloud Protector. The Cloud Protector is a trained back propagation neural network (NN), to help detect and filter out DDoS messages. A neural network is a set of connected units made up of input, hidden and output layers [12] [13]. Each of the connections in a neural network has a weight associated with it. In a neural net the focus is on the threshold logic unit (TLU). The TLU inserts input objects into an array of weighted quantities and sums them up to see if they are above the threshold.

C. Clock Drift Method

A Clock drift is used to maintain clock rates between client and server. The clock rates between the client and server adjusted and aligned. The Pseudo random function generates pseudo random seed in the server and it assigns ports to each client. The Client to send contact messages to the server. And the client align the hopping time period at adversary chosen time intervals to control align. Each client adjusts its hopping period length and aligns its hopping period with the server. Clients get the seed pseudorandom function from Server to compute the port sequence. The application data is sent from Client to Server which is sent out to the open ports of Server that changes every time units of Server clock, corresponding to client time units in Clients clock. This transpires after the contact-initiation part. Periodically, the sender and receiver can use new seeds of the pseudorandom function to generate different port number sequences. This allows the port number sequence which is used for communication is changed periodically [14]. The clients and the server share a pseudorandom function to compute which port should be used in a certain time slot. Every client uses the same pseudorandom function to generate the destination port number. A distance field can also be introduced via the use of the time-to-live value within the packet that the message comes in. With this distance field, it simplifies path reconstruction.

VI. Conclusion

DDOS attacks are quite advanced and powerful methods to attack a network system to make it either unusable to the legitimate users or demote its performance. There is greater need for solutions to overcome these attacks. In this paper, we have presented a detailed study of various DDOS attacks and its security approaches. Based on the analysis of DDOS attacks, we observe that HTTP and XML DOS attacks are the most serious threats to cloud computing. In future, we propose a desirable solution to defend XDOS attacks.

References

[1] Rajkumar,P.A., Selvakumar, “Detection of Distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fizzy systems”, Computer Communications 36(3), February (2013), Pages:303-319.

[2] Chonka, A., Xiang, Y., Zhou, W. Alessio Bonti, “Cloud security defence to protect cloud computing against HTTP-DoS and XML- DoS attacks”, Journal of Network and Computer Applications, 34(4), July (2011),pages: 1097-1107.

[3] Christos Douligeris and Aikaterini Mitrokotsa, “DDOS Attacks and Defense Mechanisms: A Classification”.

[4] Simona RAMANAUSKAITE “Modeling and research of Distributed Denial of service Attacks “. Available:http://vddb.laba.lt/fedora/get/LT-el

[5] Gilshan shrivastava and KavithaSharma,”The Detection & Defense of DOS & DDOS Attack: A Technical Overview”, Proceedings of ICC, 27-28 December 2010.

[6] B. Prabadevi , N.Jeyanthi, “Distributed Denial of Service Attacks and its effects on Cloud environment- A Survey”, The 2014 International Symposium on Networks, Computers and Communications, Pg. 1-5, IEEE Explore, 17-19 June 2014.

[7] S.S Chopade, K.U. Pandey, D.S. Bhade, “Securing Cloud Servers against Flooding Based DDOS Attacks”, International Conference on Communication Systems and Networking Technologies, Pg. 524-528, IEEE Explore 6-8 April 2013.

[8] Pourya Shamsolmoali,M.Afshar Alam et al., ”C2DF: High Rate DDOS filtering method in Cloud Computing”, International Journal of Computer Network and Information Security, 2014, 9, 43-50.

[9] K. Shanti, "A Defense Mechanism to Protect Cloud Computing Against Distributed Denial of Service Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 5, May 2013.

[10] Amit Vinayakrao Angaikar, Narendra Shekokar, Mahesh Maurya, "The Countering the XDOS Attack for Securing the Web Services", International Journal of Computer Science and Information technologies, Vol 5(3), Pp. 3907-3911,2014.

[11] Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi, "Securing Cloud Computing Environment against DDoS Attacks", International Conference on Computer Communication and Informatics, Pg. 1-5, IEEE Explore, 10-12 Jan 2012.

[12] Trostle J, (2006), "Protecting Against Distributed Denial of service attacks Using Distributed Filtering", Securecomm and Workshops, Pg. 1-11, IEEE Explore, Aug 28 2006- Sep1 2006.

[13] Iftikhar A., Azween B. A., Abdullah S.A., "Application of Artificial neural Network in Detection of DoS attacks", SIN'09 Proceedings of the 2nd international conference on Security of information and networks, Pg 229-234, ACM, New York, Oct 6-10, 2009.

[14] Zhang F U, "Multifaceted Defence against Distributed Denial of Service Attacks: Prevention, Detection, Mitigation", Ph.D. Thesis, Division of Networks and Systems, Chalmers University, 2012