DDoS ATTACKS & DEFENCE MECHANISMS AND ITS MITIGATION TECHNIQUES

Ritu Maheshwari Bansal[1], Deepika khurana[2], Ritika Bateja[3]

[1]Ph.D Scholar (Computer Science), Department of Computer Science, Barkatullah University,Bhopal, Madhya Pradesh, (India)

[2,3]Assistant professor (CSE), Faculty of Engineering & Technology, Manav Rachna International University, Faridabad, Haryana, (India)

ABSTRACT

DDoS attacks prevents legitimate users from using a victim computing system or network resource. Two main classes of DDoS attacks are: bandwidth depletion and resource depletion attacks. There are three essential components to DDoS countermeasures and based on which pro-active, post-active and location of defense based challenges have been found out. Several mitigation techniques have been analysed and discussed in this paper which can be taken as a base for further research work in the domain of mitigation of DDoS attacks at source, intermediate or at victim server side.

Keywords: ***DDoS, Defense Mechanism, Mitigation, Load Balancing, Filtering***

I. INTRODUCTION

A Denial of Service (DoS) attack is an attack that prevents legitimate users from using a victim computing system or network resource. A Distributed Denial of Service (DDoS) attack deploys many computers to launch attack to gain its purpose. It can be performed at network level, operating system level, application level and many more. In past, DDoS attack has been able to damage the companies like YAHOO, AMAZON, etc. in terms of services and finance. It is a large-scale, coordinated attack on the availability of services of a victim system or any network based resource that is launched indirectly by compromised hosts on the Internet.

In this attack, attacker fills the networks bandwidth with large amount of request packets that consumes the bandwidth and makes it difficult for the legitimate user to access the service. The attacker launch millions of machines for a DDoS attack, first scan millions of machines for vulnerable service and other weakness, then gain access and compromise these zombies or slave machines. These infected machines can recruit more zombies. When the assault starts, the real attacker hides the identity and sends orders to zombies to perform the attacks. The attackers are not going to thieve, modify or remove the information exchanged on networks, but they attempt to impair a network service, thus to block legitimate users from accessing the service. This attack is comprehensive and synchronized attack, initiated by a group of negotiated hosts upon a victim network resource. All operations like ecommerce, banking, trade, social activities and mail have now become easy on internet. To use the Internet for daily operations, increasing number of services are motivated. Internet security includes confidentiality, message integrity, non-repudiation, and authentication. Major issue is availability. DDoS attacks pose a big threat to availability of services on the Internet. Without being authenticated on the internet, any

packet can be sent to anyone. A packet that arrives to a provided service has to be processed by the receiver. Fake identity can be created by the attacker and malicious traffic can be sent.

In this paper, section II presents *Categorization of DDoS Attacks, its Architecture and Defense Mechanisms*, section III presents *DDoS Defense Mechanisms and Techniques*, section IV presents *Challenges in Defense Mechanisms* section V presents *DDoS Mitigation Techniques* and lastly, section VI presents *Conclusions*.

II. CATEGORIZATION OF DDOS ATTACKS

When a computer or a network is incapable of providing the desired services it means that Denial of Service attacks are occurred. In this, the services of the network are purposively blocked by the user. These DoS attacks doesn't cause any harm to the data but make the resources unavailable. [5]. Attack Pattern is a process to identify the view of attackers, that gives the information about the attack types, attack prerequisites, attack weaknesses, the knowledge so required to perform an attack and all the information related to the attack that had been taken place in the network [2].

Two main classes of DDoS attacks are: bandwidth depletion and resource depletion attacks [7]. A bandwidth depletion attack is created to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system. It is an activity that aims to disable the services provided by the victim by sending unwanted traffic in large volume [11]. A resource depletion is an attack that is created to hold down the resources of a victim system. This attack targets a server or process at the victim making legitimate requests for service unavailable to the users [3]. There are two major impacts of bandwidth attacks i.e. consumption of the host's resources and consumption of the network bandwidth.

III. DDOS DEFENCE MECHANISMS AND TECHNIQUES

There are three essential components to DDoS countermeasures [4]. There is the component for preventing the DDoS attack which includes preventing secondary victims and detecting and neutralizing handlers. There is the component for dealing with a DDoS attack while it is in progress, including detecting or preventing the attack, mitigating or stopping the attack, and deflecting the attack. Lastly, there is the post-attack component which involves network forensics. Based on the underlying strategies, we can categorize current DDoS detection and defense approaches into three categories: Proactive Mechanisms, Reactive Mechanisms and Post Attack Analysis [9].

3.1 Pro-Active or Preventive Defense Mechanisms

Instead of detecting the attacks by using attack pattern these mechanisms try to improve the reliability of the global Internet infrastructure by adding extra functionality to Internet components to prevent attacks and exploitation. Preventive mechanisms are the actions performed prior to an attack either to eliminate the possibility of being a target of attacks or to support the target to increase the effects of attacks sufficiently. Several preventive countermeasures are:

Planning a proper risk management strategy is a matter of preparing for attacks, determining what should be protected, how and at what cost. It is a plan of procedures that guides the responses to various attacks and the recovery of possible damages.

Load balancing refers to key services being distributed to multiple locations. Thus, if an attack is primarily engaged against a certain servers, the other servers may still be able to operate sufficiently. Acquiring

abundance of bandwidth is expensive. The aim is to acquire as much of bandwidth and other resources to retain operability even in case of a powerful attack.

Filtering of all unnecessary traffic is a method of defining the problem. Filtering of all unnecessary traffic is a precaution for protecting own hosts from being compromised.

3.2 Reactive Defense Mechanisms

These mechanisms deploy third-party Intrusion Detection Systems (IDS) to obtain attack information and take action based on this information. When IDS system detects the DDoS attack packets, filtering mechanism are then used to filter out the attack stream completely, even at the source network. If the IDS cannot detect the attack stream accurately, rate limiting is used. These mechanisms refer to the actions performed to mitigate the effects of one or more ongoing attacks and they consist of detection and response procedures.

Detection is the process of determining the target under attack, that must be detected first.

Response is the process of reaction after the detection procedure has verified that there is an ongoing attack. These methods include some form of traffic filtering. Most of the remaining responsive methods relate to tracing the approximate attack source, referred as IP-traceback.

3.3 Post-Attack Forensics or Post Active Methods

The aim is to either look for attack patterns that will be used by IDS or identify attackers using packet tracing. Packet tracing traces Internet traffic back to the true source. Post-active methods are the actions performed after an attack has occurred to mitigate the threat of DDoS. Post active methods are about tracing the attacker as well as analysing the vulnerabilities exploited by the attack and engaging into repairs. Tracing one or more attackers is a task that relies heavily on the information gathered during the attack.

The defense mechanisms, on the basis of location, can be categorized into three basic models: (1) the Victim Model (VM), a traditional defense model that identifies and filters attack traffic at a single location, the victim. (2) the Victim-Router Model (VRM), a cooperative model, that identifies and filters the attack traffic at multiple locations. The defense process is triggered by the signal from a victim and accomplished with the cooperation from participating routers. (3) the Router-Router Model (RRM) a distributed defense model that detects the attack traffic by sharing information among participating routers. Each model is classified according to the employment of the defense mechanism, and cooperation among the victim and router network components. [10]. The aim of DDoS defense is to filter attack traffic close to the attack sources so that both network and server resources will be saved.

IV. CHALLENGES IN DEFENCE MECHANISMS

4.1 Pro-Active Challenges

Proactive defense prevents the malicious packets from reaching the victim hence, they cannot impact the protected service [14]. Proactive solutions mitigate the DDoS attacks before they affect the performance of targets. The attacker can still spoof the addresses within the expected range. When the “attack army” consists of a large number of zombie machines, the attacker does not need to use IP spoofing, as each zombie machine can just flood a small volume of traffic with its own address. The aggregated malicious traffic is then, enough to overwhelm the victim network.

4.2 Post-Active Challenges

Once an attack is detected, the next response would be to block the attack traffic at its source. Unfortunately, there is no easy way to track IP traffic to its source. This is because of two aspects of IP protocol. The first is the ease with which IP source addresses can be forged. The second is the stateless nature of IP routing, where routers normally know only the next hop for forwarding a packet, rather than the complete end-to-end route taken by each packet [10].

4.3 Location of Defence based Challenges [22]

Source-initiated Challenge: Source sites are responsible for ensuring about attack-free outgoing packets. But, the viability of such approaches lies on cooperation among a majority of ingress network administrators Internet-wide.

Victim-initiated Challenge: The victim can initiate countermeasures to reduce incoming traffic. DDoS traffic is very low at sources which, is not easy to characterize attacks packets at the source [16]. Automation of real time response by generating alerts and collaborating with other defense nodes is difficult at the victim side.

4.4 Ddos Mitigation Techniques

Mitigation is the process to minimize the effect of an ongoing attack. The simplest method is to drop the packets belonging to the attacker [5]. But the problem lies in distinguishing between legitimate or illegitimate client.

Pushback [25] enables routers to congestion rate limit them by identifying high bandwidth aggregates. It requests its upstream neighbour's to help in rate limiting if the congested router cannot control the aggregate by itself. When attackers are not collocated on a path separate from the legitimate traffic, it inflicts collateral damage. It also cannot work in non-contiguous deployment and when core routers are not congested, it cannot detect attacks. Legitimate traffic can be protected by by pushing the defense frontier towards attack sources.

Selective pushback is an improved version of pushback [12]. By analyzing the traffic distribution change of all upstream routers at the target, it sends pushback messages to the routers closest to the attack sources It has two advantages. First, attack sources can be located more accurately by traffic distribution analysis as compared to volume-based approaches. Second, the pushback message can be sent to the routers closest to the attack sources directly, that can mitigate the attack damage more quickly than the original pushback scheme. But, accuracy of detection, and deployment across multiple ISP domains is an issue.

In [21] to decrease the impact of attack, designated controllers of multiple domains interact and traceback the attack path. The limitation under detecting and characterizing attack traffic is the use of third party detection. It is good to find ingress edges of attack, but attack signature should be as narrow as possible to lessen collateral damage. The communication between victim and controller and between agents and controllers should be possible in state of DDoS and should also be integral, authentic and confidential. But, single point failure due to DDoS attack at controller can damage the scene.

Filtering techniques are also used to stop the attack. If attack signatures are not accurate, adaptive rate limit would be better. To verify legitimate users and send their traffic on the overlay to secret servlets, SOS [13] uses access points (SOAPs) close to source that tunnel it to a distributed firewall protecting the victim. SOS offers good protection to the server but as it is routed on the overlay the traffic experiences a significant delay. SOS approach involves a authentication and overlay routing mechanisms and suffers from routing related drawbacks.

But, if attackers can gain massive attack power, all the SOAPs can be paralyzed, and the target's success will be disrupted.

Active Security System (ASSYST) [8] supports distributed response with nodes equivalent to classifiers being deployed only at edge networks and with non-contiguous deployment. COSSACK [6] that is deployed at source and victim networks, forms a multicast group of defense nodes and cooperate in filtering the attack. Both [1] and [20] that do not deploy their defense mechanisms cannot handle attacks from legacy networks. Parameter Based Defense [23] that rate limits an attack originated from one of its customer networks, constructs a multicast group at an ISP. It does not perform well in non-contiguous deployment and requires wide deployment. Yau et al. [15] propose a router throttle mechanism that is installed at the routers close to the victim. This defense system inflicts collateral damage to legitimate traffic by incorporating only core defense mechanisms and victim end. Some router based solutions with the aid of an overlay of routers traces and stops the attacks close to the source. Tracing inflicts collateral damage on legitimate users that share a network with an attacker which is done using signatures assigned to each source network.

DefCOM [24] can collaborate in DDoS detection and response through a dynamically-built overlay by providing added functionality to existing defenses. Three types of DefCOM functionalities are added to existing routers or defense nodes. A single physical node can host more functionality at a time. The functionalities are: (1) A classifier functionality that is capable of differentiating the legitimate traffic from the attack traffic is added to existing defenses. (2) A rate limiter functionality that runs a weighted fair share algorithm (WFSA) to prioritize traffic and forwards to the victim is deployed by routers. It rate limits this traffic to preserve victim's resources. (3) An alert generator functionality that can detect a DoS attack is added to defenses. An alert generator propagates the attack alert to other DefCOM nodes using the overlay. The alert contains the IP address of the attack's victim and specifies a desired rate limit. Extra infrastructure for overlay and cooperation at all points of the Internet are major issues. Collateral damage lies on accuracy of classifier.

Yau et al. [15] implemented router throttles to fight DDoS attacks against Internet servers. A proactive approach is followed. Routers along forwarding paths, regulate the contributing packet rates to more moderate levels before aggressive packets can converge to overwhelm a server. The mechanism to install a router throttle at an upstream router several hops away is for server. The throttle limits the rate at which packets destined for server will be forwarded through the router. Traffic exceeding the rate limit can either be rerouted to an alternate server or dropped. The throttle rate is reduced if the current throttle fails to bring down the load to below threshold. It is increased if the server load falls below a low-water mark.

ALPi, scheme with reduced implementation complexity and enhanced performance extends the packet scoring concept [17]. A leaky-bucket overflow control scheme facilitates high-speed implementation and simplifies the score computation. An attribute-value-variation scoring scheme increases the accuracy of detecting and differentiating attacks by analyzing the deviations of the current traffic attribute values.

DDoS attacks require new criteria to detect increasingly complex and deceptive assaults and hence mitigating the effects of the attack to ensure resource availability [18]. Normal Distribution is the process of finding the probability of failure, undesirable event in a large group of quantity. It is in practical, impossible to calculate and qualify all items in given specified time. Normal distribution is being used in various quantitative study to calculate large amount of such items.

In SIFF, aim is to protect privileged packets from unprivileged packet flooding, allowing packet receivers to terminate individual privileged flows selectively before arriving near the victim. For this, all network traffic is separated into privileged and unprivileged packets [19].

V. CONCLUSIONS

DDoS attacks have been categorized and it's proactive, reactive and post active defense mechanisms have been discussed. Challenging issues of these mechanisms and techniques have been found out. A number of mitigation techniques have been studied and analysed. These enable us to distinguish between legitimate and illegitimate traffic and accordingly either drop or detect the unwanted packets. This analysis work can be taken as a base for further research work in several DDoS mitigation techniques.

REFERENCES

[1] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, R. Govindan, "COSSACK: Coordinated Suppression of Simultaneous Attacks," IEEE Conference on DARPA Information Survivability, Information Sciences Institute, vol. 1, pp. 2-13, 22-24, April, 2003.

[2] A. Madhuri, A. Ramana Lakshmi, "Attack Patterns for Detecting and Preventing DDoS and Replay Attacks," International Journal of Engineering and Technology, vol. 2 (9), pp. 4850-4859, 2010.

[3] G. Zhang and M. Parashar, "Cooperative Defence against DDoS Attacks," Journal of Research and Practices in IT, vol. 38 (1), pp. 69-84, February 2006.

[4] R. Kumar, R. Karanam, R. Bobba, S. Raghunath, "DDoS Defense Mechanism," IEEE International Conference on Future Networks, VIT University, Vellore, India, pp. 254-257, 2009.

[5] D. Garg, "DDOS Mitigation Techniques-A Survey," International Conference on Advance Computing in Communication and Networks, pp. 1302-1309, 2011

[6] B.B. Gupta, R.C. Joshi, M. Mishra, "Distributed Denial of Service Prevention Techniques," IEEE International Journal of Computer and Electrical Engineering, vol. 2 (2), pp. 269-276, April, 2010.

[7] S. Liu, "Surviving Distributed Denial-of-Service Attacks," IEEE Journal on IT Professional, vol. 11 (5), pp. 51-53, 2009.

[8] R. K. Chang, "Defending against flooding-based DDoS attacks: A tutorial", IEEE Communications Magazine, vol. 40 (10), pp. 42-51, October 2002.

[9] L. Garber, "Denial-of-Service attack rip the Internet," IEEE Journal on Computer, vol. 33 (4), pp. 12-17, 2000.

[10] Tao Peng, "Defending Against Distributed Denial of Service Attacks," University of Melbourne, Doctorate Thesis, April 2004.

[11] J. Molsa, "Mitigating denial of service attacks: A tutorial," Journal on Computer Security, vol. 13, pp. 807-837, 2005.

[12] T. Peng, C. Leckie, K. Ramamohanarao, "Defending against distributed denial of service attack using selective pushback," 9th IEEE International Conference on Telecommunications, pp. 411-429, 2009.

[13] A.D. Keromytis, V. Misra, D. Rubenstein, "SOS: An Architecture For Mitigating DDoS Attacks," IEEE Journal on Selected Areas in Communication, Columbia University, New York, USA, vol. 22 (1), pp. 176-188, January, 2004.

[14] Z. Fu, "Multifaceted Defense against Distributed Denial of Service Attacks: Prevention, Detection, Mitigation," Chalmers University of technology, Sweden, Doctorate Thesis, 2012.

[15] D.K.Y. Yau, J.C.S. Lui, F. Liang, Y. Yam, "Defending against distributed denial of service attacks with Max-Min fair server-centric router throttles," 10th IEEE International Workshop on Quality of Service, Purdue University, USA, pp. 35-44, 2002.

[16] M. Sachdeva, G. Singh, K. Kumar, and K. Singh, "A comprehensive survey of distributed defense techniques against DDoS attacks," International Journal of Computer Science and Network Security, vol. 9 (12), pp. 7-15, December, 2009.

[17] P.E. Ayres, Huizhong Sun, H. Jonathan Chao, "ALPi: A DDoS Defense System for High-Speed Networks," IEEE Journal on Selected Areas in Communications, vol. 24 (10), pp. 1864-1876, October 2006.

[18] V. Shyamala Devi, Dr. R. Umarani, "Thwarting Distributed Denial of Service attacks using Normal Distribution and Weibull Theorem," International Journal of Engineering Research & Technology, vol. 1(6), pp. 1-12, August, 2012.

[19] A. Yaar, A. Perrig, D. Song, "SIFF: A stateless internet flow filter to mitigate DDoS flooding attacks," IEEE Symposium on Security and Privacy, Carneggie Melon University, Pittsburgh, USA, pp. 130-143, 9-12, May 2004.

[20] R. Canonico, D. Cotroneo, L. Peluso, S.P. Romano, G. Ventre, "Programming Routers to Improve Network Security," OPENSIG Workshop on Next Generation Network Programming, 2001.

[21] U.K. Tupakula, V. Varadharajan, "A controller agent model to counteract DoS attacks in multiple domains," 8th IFIP/IEEE International Symposium on Integrated Network Management, Macquarie University, Australia, pp.113-116, 24-28, March, 2003.

[22] Yoohwan Kim, Wing Cheong Lau, Mooi Choo Chuah, H. Jonathan Chao, "PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks," IEEE Transaction on Dependable and Secure Computing, Nevada University, Los Vegas, vol. 3 (2), pp.141-155, April-June 2006.

[23] S. Chen, Q. Song, "Perimeter-Based Defense against High Bandwidth DDoS Attacks," Transactions on Parallel and Distributed Systems," IEEE Transaction on parallel and Distributed Systems, Florida University, USA, vol. 16 (6), pp. 526-537, June, 2005.

[24] G. Oikonomou, J. Mirkovic, P. Reiher, M. Robinson, "A Framework for a Collaborative DDoS Defense," 22nd IEEE Annual Conference on Computer Security Applications, delaware University, Newark, pp. 33-42, December, 2006.

[25] J. loannidis, S.M. Bellovin, "Implementing Pushback: Router-Based Defense against DDoS Attacks," 2002, [Online]. Available: https:// www.cs.columbia.edu /~smb / papers/ pushback-impl.pdf