DDoS Attack Prevention and Mitigation Techniques - A Review

Deepika Mahajan
Shaheed Bhagat Singh State Technical Campus,
Ferozpur, Punjab, India

Monika Sachdeva
Shaheed Bhagat Singh State Technical Campus,
Ferozpur, Punjab, India

ABSTRACT

The present era is completely dependent on Internet. Internet serves as a global information source for all users, so the availability of internet is very important. In this paper the main focus is on the DDoS attack which hinders the network availability by flooding the victim with high volume of illegitimate traffic usurping its bandwidth, overburdening it to prevent legitimate traffic to get through. Various techniques to prevent and mitigate these attacks along with their advantages and disadvantages are also discussed.

General Terms

DDoS Attack, Flooding Attack, Distributed, Attacker

Keywords

DDoS attack, Availability, Zombie, Botnet.

1. INTRODUCTION

The internet in simple terms is defined as an interconnected system of computer networks. The scope of internet in day to day life is vast; it provides a wide range of information, services, resources which allows all sectors to be well linked As the need of internet is growing with time, various issues related to its security comes insight. The reason for internet insecurity is basically its design because foremost concern was its functionality rather than its security. Hence several types of attacks and threats are reason for apprehension towards security of internet. The issues related to internet security are authentication, integrity, availability, confidentiality and non- repudation. In this paper main focus is on insecurity to availability, availability means that the information, the computing systems, and the security controls are all accessible and operable in committed state at some random point of time [1]. Among all attacks DDoS (Distributed Denial of service) attacks are those which hinder clients, users to access all advantages of services available to them from server side. DDoS attack results in long system timeouts, lost revenues, large volumes of work to identify attacks and to prepare adequate response measures [23] Denial of service (DoS) attack is Distributed Denial of service (DDoS) attack since it is launched concurrently to numerous machines. DDos attacks are not new disturbance to internet, they came back late in August 1999 and after that incessantly their severity is growing. Some recognized DoS attacks are SYN Flood, teardrop, smurf, ping of death [2]. There have been large scale attacks targeting many high profile websites [26, 27, 28]. These sites include twitter, facebook, Amazon etc. There are varieties of DDoS attacks as classified in [16, 17]. However, the most common form of DDoS attacks is a packet-flooding attack, in which a large number of seemingly legitimate TCP, User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP) packets are directed to a specific destination. DDoS attacks cannot be detected and stopped easily because forged source addresses and other techniques are used to conceal attack sources [29]. As per Peng et al. [19], protection against these attacks is challenging for mainly two reasons. First, the number of zombies involved in a DDoS attack is very large and exploitation of these zombies spans large geographical areas. The volume of traffic sent by a single zombie might be small, but the volume of aggregated traffic arriving at the victim host is overwhelming. Second, zombies usually spoof their IP addresses under the control of attacker, which makes it very difficult to trace the attack traffic back even to zombies. In this paper an overview of DDoS attack and various prevention and mitigation techniques for DDos attacks along with their advantages and disadvantages is discussed.

2. OVERVIEW OF DDOS ATTACK

A denial-of-service attack is regarded as an attempt to prevent the legitimate use of a service. A distributed denial-of-service attack differs from DoS attack as it deploys multiple attacking entities to attain this goal. One frequently exercised manner to perform a DDoS attack is for the attacker to send a stream of packets to a victim; this stream consumes some key resource, thus rendering it unavailable to the victim's legitimate clients. Another common approach is for the attacker to send a few malformed packets that confuse an application or a protocol on the victim machine and force it to freeze or reboot [17]. DDoS attack causes a failure of service to users, loss of network connectivity and facility by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

DDoS attack does not rely on particular network protocol or system weakness. It simply exploits the huge resource asymmetry between the Internet and the victim [3]. Since Internet architecture is open in nature, any machine attached to it is publically visible to another machines attached to enable the communication. The hacker or attacker community takes the unhealthy advantage of this open nature to discover any insecure machine connected to the Internet. The discovered machine is thus infected with the attack code. The infected machine can further be used to discover and infect another machine connected and so on. The attacker thus gradually prepares an attack network. Depending upon the attacking code the hackers send control instructions to masters which in turn control agents. The zombies under the control of masters transmit attack packets which converge at victim to exhaust its resources. DDoS attack basically targets victim's computational or communicational resources [18], such as bandwidth, memory, CPU cycle, file descriptors and buffers etc. The recruit phase is very first phase in occurrence of DDoS attack in which the attacker discovers the vulnerability in the victim system and recruit multiple agents, these multiple agents also called as bots or zombie. These zombies form a botnet including all such negotiated machines which are responsible to run attack code under common command and control by the attacker. The second phase is the exploit phase in which the vulnerability is exploited in the recruited zombies. The third phase known as infect phase bots are

infected with the attack code. Last phase is the use phase which uses the agents to send the attack code to victim system.

Mirkovic et al. [17] have classified DDOS attacks into two broad categories: flooding attacks and vulnerability attacks. Flooding DDoS attacks consume resources such as network bandwidth. These attacks flood the network with such a high volume of traffic which consumes their available network resources are and legitimate user requests cannot get through, resulting in degraded productivity. Vulnerability attacks use the expected behavior of protocols such as TCP and HTTP to the attacker's advantage. Connectivity attacks flood a computer with such a high volume of connection requests, that all available operating system resources are consumed and the computer can no longer process legitimate user requests [25]. However, resources of connecting network are not a problem in case of commercial servers as these are hosted by the ISPs. But server resources such as processing capacity, buffer limit etc., are put under stress by flood of seemingly legitimate requests generated by DDoS attack zombies. Each request consumes some CPU cycles. Once the total request rate is more than the service rate of server, the requests start getting buffered in the server, and after some time due to buffer over run, incoming requests are dropped. The congestion and flow control signals force legitimate clients to decrease their rate of sending requests, whereas attack packets keep coming. Finally, a stage comes when only attack traffic is reaching at the server. Thus, service is denied to legitimate clients [2]. Robinson et al. [20] stated that as attack strength grows by using multiple sources, the computational requirements of even filtering traffic of malicious flows become a burden at the target.

3. DDOS DEFENSE

DDoS defense means to relieve victim's resources from high volume of fake packets sent by attackers from disseminated locations, so that these resources could be used to serve legitimate users. The distributed nature of DDoS attacks make them enormously difficult to combat. Attackers may also use IP spoofing to conceal their identity. There is no satisfactory security in comparison to persistent security breaches in the Internet. DDoS defense mechanism consists of prevention, detection, tolerance and mitigation and response.

According to, Douligeris et al. [16]Attack prevention aims to fix security holes, such as insecure protocols, weak authentication schemes and vulnerable computer systems, which can be used as stepping stones to launch a DoS attack. This approach aims to improve the global security level and is the best solution to DoS attacks. Various methods of prevention are ingress filtering, egress filtering, route based packet-filtering, history based IP-filtering. Detection means a host computer and a network can guard themselves against being a source of network attack as well as being a victim of a DDoS attack either by using the database of known signatures or by recognizing anomalies in system behaviors. It is impossible to completely stop DDoS attacks, so mitigation and tolerance is important. The impact of attack can be minimized through fault tolerance or increasing quality of service. The table 1 [11-15] and [21-24] underneath discusses various prevention techniques and table 2 [4-9] discusses various mitigation and tolerance techniques to combat DDoS attacks.

Table 1. DDoS prevention Techniques

Name of Technique	Approach Used	Advantage	Disadvantage
Ingress Filtering	Ingress Router set to drop traffic with IP address not matching to domain prefix.	Reduces DoS attack due to IP spoofing , locates source of attack if ISP's have ingress filtering instead of customer links	It just reduces, does not prevent use of forged source address of another host within permitted prefix filter range.
Egress Filtering	Makes certain that only assigned IP address space leaves the network. Outbound filter is used.	Protects other domain from possible attack	There is wastage of resources of domain where packet originates
Route Based Distributed Packet Filtering	Uses routing information. It works on basis that for every link in internet, there is limited number of source IP addresses from which traffic comes.	Synergistic filtering effect is possible, spoofed IP flows are prevented from reaching other Autonomous Systems.	Difficult to update route-based filters in real time. Acquiring global knowledge of whole n/w topology has scalability issues
History Based IP-Filtering	A pre-built IP address database is used and an edge router acknowledges the incoming packets accordingly.	It is robust, there is no need of studying the whole network topology	If the invader knows that the IP packet filter is based on prior connections, they might deceive the server to be included in the IP address database.
Secure Overlay Services (SOS)	Hash based routing is used, the user traffic is authenticated via SOAP then traffic is routed though small number of nodes called as servlets to victim.	Distributed system that offers exceptional protection to the specified target at the cost of modifying client systems.	Not recommended for public servers.
Load Balancing	Simple approach that enables network providers to	In a multiple-server architecture the	It is costly and complex.

	increase the provided bandwidth on critical connections and prevent them from going down in the event of an attack.	balance of the load is necessary so that both the improvement of normal performance.	
Honey pot	Allow the attacker to attack the honypot and not the actual system; they also help to gain info of the attacker by storing their records, the type of attack and type of software used.	Main goal is to make attacker think that he has compromised the machine(honeypot) as slave and understand the attack code, this helps to detect the attacker	Assumes that the attack must be detectable using signature based detection tools.

Table 2. DDoS Mitigation and Tolerance Techniques

Name of Technique	Approach Used	Advantage	Disadvantage
Integrated Intserv	Uses the Resource Reservation Protocol (RSVP) to manage the resources allocation along the path that a particular traffic passes.	The bandwidth and buffer space for a particular link is assured for specific traffic flow	Due to pre allocation of resources their consumption increases.
Differentiated Services	Based on Type of Service byte in IP header	Allocates resources based on TOS of incoming packet	Requires cooperation of multiple administrative domains.
Class Based Queuing	Queues for different type of packets and different packets for different type of service is set, bandwidth is assigned to queues	Maintains QoS during DDoS attack	It is difficult to maintain queues.
Resource Pricing	propose a distributed gateway architecture and a payment protocol that imposes dynamically changing prices on both network, server, and information resources	They identify allotting a priority mechanism to desirable clients as being key, and punish clients that cause load on the server.	Malicious user can populate the system with fake requests at low price, thus driving up the price for legitimate users.
PushBack	First, a local Aggregate Congestion Control (ACC) detects the congestion at the router level and devises an attack signature. The signature defines a traffic aggregate as a group of traffic flows with a common property Then, a local ACC determines an appropriate rate limit for this aggregate.	PushBack can effectively mitigate DDoS attacks when the attacker's machines are gathered in few places.	When attackers are widely distributed over the Internet, the legitimate traffic also is rate-limited and PushBack will not be successful.
Throttling	Traffic passing through the router to the source is rate limited to the throttle rate. only aggressive flows which do not respect their rate shares are punished and not other flows. This method is still in the experimental stage.	Prevents servers from going down. Eg: web servers	Difficult to implement throttling, hard to decipher legitimate traffic from malicious traffic. In the process of throttling, legitimate traffic may sometimes be dropped or delayed and malicious traffic may be allowed to pass to server.

3. CONCLUSION

In this paper, an apparent vision of the DDoS attack is attained and discussed numerous techniques along with their pros and cons to prevent and alleviate these attacks. Due to an alarming increase in DDoS attacks, internet security from these attacks becomes vulnerable issue. Having clarified view of the attack, effective countermeasures can be implemented to fight against these attacks.

4. REFERENCES

[1] Tipton H. and Krause M. 2004, Information Security Management Handbook, CRC Press.

[2] Sachdeva M., Singh G., Kumar K. and Singh K. 2010. DDoS incidents and their impact: A review, International Arab Journal of Information Technology, vol. 7, Issue 1, pp. 14-19.

[3] Chang R.K.C. 2002. Defending against flooding-based distributed denial-of-service attacks: A Tutorial, Computer Journal of IEEE Communication Magazine, vol. 40, Issue 10, pp. 42-51.

[4] Yau D.K., Lui J.C.S., Liang F. 2002. Defending Against Distributed Denial of Service attacks with max–min fair server-centric router throttles, in: Proceedings of the Tenth IEEE International Workshop on Quality of Service (IWQoS), Miami Beach, FL, pp. 35–44.

[5] Zhao W., Olshefski D., Schulzrinne H. 2000. Internet Quality of Service: an overview, Columbia Technical Report CUCS-003-00.

[6] Blake S., Black D., Carlson M., Davies E., Wang Z., Weiss W. 1998. An architecture for differentiated services, in: IETF, RFC 2475.

[7] Geoffrey M.B., Xie G. 2002. A feedback mechanism for mitigating Denial of Service attacks against differentiated services clients, In Proceedings of the 10th International Conference on Telecommunications systems, Monterey, CA, pp. 204–213.

[8] Ioannidis J., Bellovin S.M. 2002. Implementing pushback: router-based defense against DDoS Attacks. In Proceedings of Network and Distributed System Security Symposium, (NDSS), San Diego, CA, pp. 6–8.

[9] Mankins S.M., Sangpachatanaruk C., Znati T., Melhem R., Moss D. 2003. Proactive server roaming for mitigating Denial of Service attacks. In Proceedings of 1st International Conference on Information Technology Research and Education (ITRE), Newark, NJ, USA, August 10–13,.

[10] Kargl F., Maier J., Weber M. 2001. Protecting web servers from Distributed Denial of Service attacks. In Proceedings of the Tenth International Conference on World Wide Web, Hong Kong, pp. 514–524.

[11] Ferguson P., Senie D. 2001. Network ingress filtering: defeating Denial of Service attacks which employ IP source address spoofing. In RFC 2827.

[12] Global Incident analysis Center—Special Notice—Egress filtering, Available from <http://www.sans.org/y2k/egress.htm>.

[13] Park K., Lee H. 2001. On the effectiveness of route-based packet filtering for Distributed DoS attack prevention in powerlaw Internets, In Proceedings of the ASIGCOMM_01 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press, New York, pp. 15–26.

[14] Peng T., Leckie C., Ramamohanarao K. 2003. Protection from Distributed Denial of Service attack using history-based IP filtering. In Proceedings of IEEE International Conference on Communications, Anchorage, AL, USA.

[15] Keromytis A., Misra V., Rubenstein D. 2002. SoS: secure overlay services. In Proceedings of the ACM SIGCOMM_02 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press, New York, pp. 61–72.

[16] Douligeris C. and Mitrokotsa A. 2004. DDoS Attacks and Defense Mechanisms: Classification and State of the Art, Computer Journal of Networks, vol. 44, Issue 5, pp. 643-666.

[17] Mirkovic J., and Reiher P. 2004, A taxonomy of DDoS attack and DDoS defense mechanisms, Computer Journal of ACM SIGCOMM, vol. 34, Issue 2, pp. 39-53.

[18] Kumar K., Joshi R., and Singh K. 2006, An integrated approach for defending against distributed denial of service attacks, IIT Madras. [Online]. Available: http://www.cs.iitm.ernet.in/~iriss06/paper.html.

[19] Peng T., Leckie C., and Ramamohanarao K. 2007, Survey of Network Based Defense Mechanism Countering the DoS and DDoS Problems, Computer Journal of ACM Computing Surveys, vol. 39, Issue 1, pp. 123-128.

[20] Robinson M., Mirkovic J., Schnaider M., Michel,S., and Reiher P. 2003, Challenges and Principles of DDoS Defense, Computer Journal of ACM SIGCOMM, vol. 5, Issue 2, pp. 148-152.

[21] Lee R.B., Taxonomies of Distributed Denial of Service networks, attacks, tools and countermeasures, Princeton University, Available from <http://www.ee.princeton.edu/~rblee>.

[22] Weiler N. 2002. Honeypots for Distributed Denial of Service, In Proceedings of the Eleventh IEEE International Workshops Enabling Technologies: Infrastructure for Collaborative Enterprises 2002, Pitsburgh, PA, USA, pp. 109–114.

[23] Golubev V. 2005. DoS attacks: crime without penalty[Online]. Available: http://www.crime- research.org/ articles/1049/

[24] Sardana A., Joshi R. 2009. An auto-responsive honeypot architecture for dynamic resource allocation and QoS adaptation In DDoS attacked network, Computer Communication on Heterogeneous Networking for Quality, Reliability, Security, and Robustness – Part II Elsevier, vol. 32, Issue 12, pp. 1384- 1399.

[25] Stein L.D., Stewart J.N. 2002. The World Wide WebSecurity FAQ, version 3.1.2 , Available from <http://www.w3.org/Security/Faq>.

[26] CERT Coordination Center, Denial of Service attacks, Available<http://www.cert.org/tech_tips/denial_of_service.html>.

[27] Computer Security Institute and Federal Bureau of Investigation 2001, CSI/FBI Computer crime and security survey, CSI, Available from <http://www.gocsi.com>.

[28] Moore D., Voelker G., Savage S. 2001. Inferring Internet Denial of Service activity, In Proceedings of the USENIX Security Symposium, Washington, DC, USA , pp. 9–22.

[29] Yuan J., Mills K. 2005. Monitoring the macroscopic effects of DDoS flooding Attack, IEEE Transactions on Dependable and secure computing, vol. 2, Issue. 4, pp 324-335.