Mitigation of Distributed Denial of Service (DDoS) Threats

Abhilash C. S.
Student
M-Tech Computer science and Engineering,
MES College of Engineering, Kuttipuram.

Sunil kumar P. V.
Assistant Professor
Department of Computer science and Engineering
MES College of Engineering, Kuttipuram.

ABSTRACT
Denial of Service (DoS) attacks is a kind of attacks against computers connected to the Internet. The goal of DoS attacks is to keep away authorized users from accessing resources. The infected computers may crash or disconnect from the Internet. The distributed denial of service (DDoS) attack is a continuous critical threat that has caused severe damage to servers and will cause even greater intimidation to the development of new Internet services. In the present scenario the mitigation of these attacks has most importance. There are a number of mitigation techniques have been proposed by various researchers. A Web Referral Architecture for Privileged Services (WRAPS) proposed by the authors [8], that can mitigate the DDoS attack that plague website today. It allows a legitimate client to obtain a privileged URL by a referral hyperlink, from a website trusted by the target website. There are several limitations are present in this architecture. WRAPS support only clients that use fixed IP address, instead of as domain names it encodes privileged URLs as IP addresses. If the users want privileged services, then they must access the target site through privileged URL. That means the domain name of server not resolved via DNS and the users must save their privileged URL from the server when it is updated at the end of a privileged period, thus WRAPS not transparent to users.

1. INTRODUCTION
Denial-of-Service (DoS) attacks is a major threat to Internet security. Denial-of-service attacks can essentially disable computers or networks. Depending on the nature of the enterprise, this can effectively disable the organizations. Some denial-of-service attacks can be executed with limited resources against a large, sophisticated site. For example, an attacker with an old PC and a slow modem may be able to disable much faster and more sophisticated machines or networks. A new kind of DoS attacks is Denial-of-Capability (DoC), which takes place in the connection-setup step when clients send requests for capabilities. Distributed Denial of Service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a target system.

1.1 Types or levels of DoS attacks

1.1.1 Bandwidth Attacks
There takes certain time to load any site. Loading means it appears on the screen with the images and texts. This loading consumes some amount of memory. Every site is given with a particular amount of bandwidth by its hosting, say for example 100 GB. Now if there get more visitors who consumes all 100GB bandwidth, the hosting of the site can ban the site. So now if the attackers do the same. They can open 100 pages of a site and keep on refreshing and consume all the bandwidth and it is out of service.

1.1.2 Logic Attacks
Logic attacks exploit security vulnerabilities to cause a server or service to crash or significantly reduce performance. These attacks will be evaluated based on their effect on the network infrastructure and critical network services (Domain Name Server (DNS), Border Gateway Protocol (BGP), etc.).This is the most advanced type of attack because it involves a sophisticated understanding of networking. A classic example of a logic attack is a LAND attack, where an attacker sends a forged packet with the same source and destination IP address. Many systems are unable to handle this type of confused activity and subsequently crash.

1.1.3 Protocol Attacks
Exploiting a specific feature or implementation bug of some protocol installed at the victim in order to consume excess amounts of its resources. Protocols here are rules that are to be followed to send data over network. Popular protocol attacks are SYN attack, smurf attack, fraggle attack etc. SYN flood is an asymmetric resource starvation attack in which the attacker floods the victim with TCP SYN packets and the victim allocates resources to accept perceived incoming connections. Smurf is an asymmetric reflector attack that targets a vulnerable network broadcast address with Internet Control Message Protocol (ICMP) echo request packets and spoofs the source of the victim. Fraggle is a variant of smurf that sends UDP packets to echo or chargen ports on broadcast addresses and spoofs the source of the victim.

1.2 Distributed Denial of Service attack (DDoS)
DDoS stands for Distributed Denial of Service attack. It is a form of attack where a lot of zombie computers (infected computers that are under the control of the attacker) are used to either directly or indirectly to flood the targeted server(s) victim, with a huge amount of information and choke it in order to prevent legitimate users from accessing them (mostly web servers that host websites). In most cases, the owners of the zombie computers may not know that they are being utilized by attackers. In some cases, there is only a periodic flooding of web servers with huge traffic in order to degrade the service, instead of taking it down completely. There are two types of DDoS attacks: First the attacks that target the network (Internet bandwidth) and choke the Internet bandwidth used by the victim server, so that it cannot accept legitimate requests coming from genuine users through the Internet gateway, Next the attacks that target the vulnerabilities in applications in order to cripple server resources like CPU (central Processing Unit), RAM (Random Access Memory), Buffer memory, etc and make the servers unavailable for handling any legitimate requests.

One step ahead, DDoS is capable of doing more harm. With this attacker can use the victim's system to infect other connected systems or send a spam. Attacker can find a weakness in the system and can inject software which can be remotely used. Using this now attacker can make the server a slave and send spams or get access to files using its permission. Thousands of system can be targeted from a single point. When used for this purpose one can see a propagating effect which multiplies. This one machine can infect other thousands of machine thus turning several megabytes of traffic to several gigabytes. This sudden increasing flow can crash down any server.

1.2.1 Components and Architecture diagram of a Distributed Denial of Service attack

As see in the Figure 1, there are mainly five components for a DDoS attack. Two of them are always there the attacker or master computer from where the attacks are initiated and the victim or attacked server which comes under the attack. Presence of just these two components makes it a Denial of Service attack (DOS). The three components in the middle, make it a Distributed Denial of Service attack, zombies are the computers from which the DDoS attacks are carried out. They may either be volunteer computers or in most cases, infected computers of internet browsing users who download certain malicious software unawares which entitle them to be controlled by the attackers. There may be an additional layer of handlers which issue instructions to the zombies and a reflector layer those amplifies the number of requests that arrive from zombies, and sends it to the victim servers to cripple it.

The architecture that proposes to protect websites against DDoS attacks is the web referral architecture for privileged service or WRAPS [1]. The web is a complicated referral graph, in which a node (website) refers its visitors to others through hyperlinks. WRAPS is a capability based approach rather than overlay based approach and all existing capability-based approaches require modifications to client-side software, but in the case of WRAPS there does not require installing anything on a Web client. WRAPS requires modifying edge routers to add mechanisms for capability verification and address translation. But compared with other capability-based techniques, this approach does not require changes to core routers and clients, and therefore could be easier to deploy than other techniques.

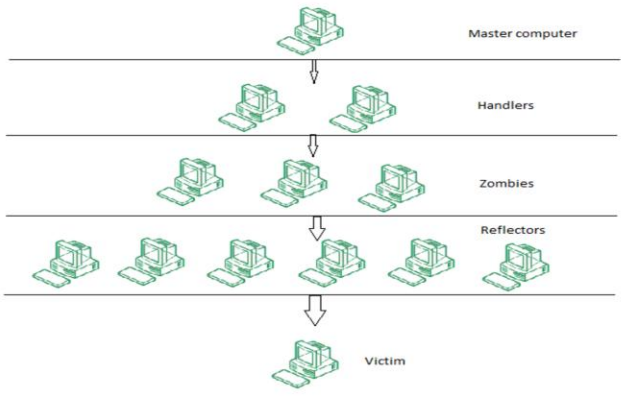

Figure 1 : Components and Architecture diagram of DDoS

2. LITERATURE SURVEY

The survey provides a historical view and uncovers gaps in existing research. The sophistication of the DDoS attack tools has kept on improving with time. Therefore a historical study of DDoS attacks also gives a good overview of the various techniques that are used in orchestrating such attacks.

W. J. Blackert et. al [1] This paper provides an overview of the DDoS-DATA project and discusses analysis results for the Proof of Work, Rate Limiting and Active Monitor mitigation technologies considered both individually and when deployed in combinations. The goal of DDoS-DATAs is to use analysis to quantify how well mitigation technologies work, how attackers can adapt to defeat these technologies and how different it can be combined. There are a different types of options are available for analyzing computer network attacks and mitigation strategies. One of them is closed form analysis and another one is real world test bed. The former one may be the most desirable form, but it requires many simplifying assumptions. But the later one is an excellent approach to understand attack dynamics. In this paper the authors presented analysis results for a 500+ node target network, three mitigation technologies and a specific attack scenario. In this paper the DDoS-DATA is examining the relationship between mitigation technologies and computer network attacks. By using the analysing methods, the authors developed a detailed understanding of the interaction between DDoS mitigation technologies and attackers.

Abraham Yaar et. al [2] developed Pi: A Path Identification Mechanism to Defend against DDoS Attacks. Pi has many unique properties one of them, it is a per-packet deterministic mechanism: each packet traveling along the same path carries the same identifier. They used trace route maps of real Internet topologies to simulate DDoS attacks and validate their design. This model consists of two phases: The learning phase and the attack phase. Pi Marking Scheme: They present a Pi Marking Scheme that should deploy on the internet routers, this section contains the sub-parts they are Basic Pi Marking Scheme, IP Address Hashing, Edge Marking in Pi, and Suppressing nearby Router Markings. The basic marking scheme is a simplest marking scheme; they proposed an n-bit scheme where a router marks the last n bits of its IP address in the IP Identification field of the packets it forwards. then break the fields in to 16/n different marking sections and use its modulo as the index in to the section of the field mark.

Filtering Schemes: The Pi filter has many uses that detect the spoofed IP addresses. The main filtering schemes are TTL unwrapping and Threshold Filtering. The attacker can modify the initial TTL of its packets to have the first hop router start marking in any one of the 16/n sections of the IP Identification field. The victim server can examine the TTL value and use it to find the oldest marking in the packet after it receives a packet. The victim can use this value to unwrap the bits of the packet by rotating them thus the oldest marking is always in the most significant bit position. There is no matter what initial value the attacker chooses for its packets TTL, the markings are always justified so that the oldest marking in the packet appears in a constant location. This is called TTL Unwrapping. In the filtering strategy one type of attack is the Marking Saturation attack, here a large number of attackers spread throughout the Internet all send packets to a single victim in the hope of having the victim classify every marking as an attacker marking, and thus drop all incoming packets. A common solution in proposed systems is a traceback mechanism that contains information of routers

mark on packets en-route to the victim, who can then use that information to reconstruct the path that the packets take from the attacker through the Internet, despite IP address spoofing.

Cheol Joo Chae et. al[3] developed IP Packet Marking . Here the IP Packet Marking, the proposed approach including node append, node sampling and edge sampling. The intermediate routers mark the IP Packets with additional information, thus the victim can easily traceback the source of such attack packets. The node sampling approach can reduces the overhead by the probabilistic marking of IP packets. The edge sampling approach marks an edge of the network topology instead of just the node. Messaging: In the messaging techniques the router information about the next node contain propose that ICMP message chase techniques IETF as techniques has to create and transmit representative. In ICMP message chase techniques router ICMP station chase mallet for creating the destination address of packet to be transmitted and middle system takes advantage of information that is collected if attack is detected collecting relevant information and chase station.

The IP Traceback system creates iTrace message and send it to the destination system. Then the destination system analyzes the iTrace message for an attack. If the system detected any attack then the destination system collects relevant information. Thus the destination system can traceback attacker using collected relevant information.The main iTrace System contains two subsystems are agent system and sever system. The agent system creates iTrace Message and sends to server system. If there is any abnormal traffic phenomenon happens it will report agent system, and detects system problem, in case of problem occurrence the information of relevant system and its Source IP is provided to the server system.

Zhenhai Duan et. al [4] Developed Controlling IP Spoofing through Interdomain Packet Filters, Here the IDPFs can independently be deployed in each autonomous system (AS) and they are deployed at the border routers so that IP packets can be inspected before they enter the network. By deploying IDPFs, an autonomous system constrains the set of packets that a neighbor can forward to the AS, a neighbor can only successfully forward a packet to the autonomous system after it announces the reachability information of all other packets are identified to carry spoofed source addresses and are discarded at the border router of the AS. In the worst case, even if only a single AS deploys IDPF and spoofed IP packets can get routed all the way to the AS in question, using an IDPF perimeter makes it likely that spoofed packets will be identified and blocked at the perimeter. That is if the AS is well connected, launching a DDoS attack upon the perimeter itself takes a lot more effort than targeting individual hosts and services within the AS. In general, by deploying IDPFs, an AS can also protect other ASs to which the AS transports traffic. It can similarly be understood that an IDPF node limits the set of packets forwarded by a neighbor and destined for a customer of the AS. IDPF finds a set of feasible paths instead of one best route, its performance will not be as good as the ideal route based filters.

Vrizlynn L. L. Thing et. al [5] In this paper DDoS responses classified by the authors as Trace back, Containment Reconfiguration, Redirection, Filtering, Rate limiting, Resource replication, Legitimacy testing, and Attackers resource consumption. They analyzed and discussed the reasons to carry out specific actions under each response type, and they considered and decided on the responses necessary to effectively mitigate DDoS TCP SYN and UDP flooding attacks. Trace back is essential in any DDoS defense system to locate nearest attack sources to perform mitigation from attacks in networks. They implemented a novel trace back mechanism in Distributed denial-of-service Adaptive ResponsE (DARE), Non-Intrusive IP Trace back, which resolves the problems in the existing mechanisms, as require wide spread deployment on Internet routers and the provision of an attack signature for identifying attack packets to extract trace back information.

M.Nagaratna et. al [6] developed Encrypted Marking based Detection And Filtering mechanism for Detecting and Preventing IP-spoofed DDoS Attacks. Here the proposed scheme is Encrypted Marking based Detection And Filtering (EMDAF). The particular encryption mechanism system has the functions, first the server receives packets from client that each packet contains source IP address and its marking value. Then the server send echo message to source IP address to verify the marking value. If both marking values are same, then server will generate a key. Else the sever identify that it is an attacked packet. Then the server will discard the request. Now using the encryption mechanism the server will encrypt the generated key. The encrypted marking will be used for secure transmission. They proposed a firewall based novel scheme that it can distinguish the attack packets by the marking value with each sent packet and thus filter out the most of the attacked packets.

Suriadi Suriadi et. al [7] developed Validating Denial of Service Vulnerabilities in Web Services. The web is more complicated with millions of websites interlinked together. The web services (WS) applications has the benefits as enterprise integration, provides exibility, and allows applications to be dynamically composed from separate services but it also introduce additional complexities. The clearest definition which defense DoS as the prevention of authorized access to resources or the delaying of time critical operations. There are a few tools available to mitigate the DoS attacks in Web Services. A Web service is a method of communication between two electronic devices over a network. Web Services were intended to solve three main problems, that is Firewall Traversal, Complexity, and Interoperability. The World Wide Web Consortium (W3C) defense a Web service as a software system designed to support interoperable machine-to-machine interaction over a network. The WS-provider processes the request and returns the response. The request and response formats are described in the web services description language (WSDL) service metadata.

DoS in Web Services: Web services are the most attractive target for hackers because even a pre-school hacker can bring down a server by repeatedly calling a web service which does expensive work. Ajax Start Pages like Page fakes are the best target for such DOS attack because if you just visit the homepage repeatedly without preserving cookie, every hit is producing a brand new user, new page setup, new widgets and what not. The first visit experience is the most expensive one. Nonetheless, it is the easiest one to exploit and bring down the site. The distributed denial of service (DDoS) attack is that it usually consists of a large number of attackers, each requesting a service from the victim. As it processes the flood of requests, the service will inevitably use up more resources. The term baseline behavior is used to indicate the level of resources being consumed by the server when it receives a large number of legitimate requests. Using this as a control, then the attackers can send the same number of requests, but this time with a malicious payload. If the use of resources by a

particular web service increases significantly when under attack as compared to its baseline behavior, this implies that the attack exposes a DoS vulnerability.

XiaoFeng Wang and Michael K. Reiter [8] developed a Web Referral Architecture for privileged services (WRAPS) enables clients to circumvent a very intensive flooding attack against a website, and imposes reasonable costs on both edge routers and referral websites. There are two approaches that are overlay-based and capability based. WRAPS differs from overlay-based approaches in several important ways it follows the capability based. First, these approaches assume the existence of an overlay need to modify protocols and client-side software. This could introduce substantial difficulties for deployment. WRAPS, however, asks only referral websites to over a very lightweight referral service, which allows WRAPS to take advantage of existing referral relationships on the web to protect important websites. WRAPS also alters neither protocols nor client software. Second, overlay routing could increase end-to-end latency, though such overheads can be significantly reduced using techniques such as topology aware overlays, and multipath overlays. In contrast, WRAPS does not change packets routing paths and thus avoids these overheads. An advantage of overlay-based approaches is that they do not need to modify edge routers. A limitation of WRAPS is that it requires modifications to edge routers, as many capability-based approaches do. However, unlike those approaches, WRAPS does not require installing anything on a Web client.

WRAPS elements planted in the standard IP forwarding path are illustrated in Fig. 2, they added five elements: IPClassifier, IPVerifier, IPRewrite, Priority queue, and PrioSched. IPClassifier classifies all inbound packets into three categories: packets addressing the websites privilege port 22433 which are dropped, TCP packets which are forwarded to IPVerifier, and other packets, such as UDP and ICMP, which are forwarded to the normal forwarding path. IPVerifier verifies every TCP packets capability token embedded in the last octet of the destination IP address and the 2-octet destination port number. Verification of a packet invokes the MAC over a 5-byte input (four for IP, one for other parameters) and a 64-bit secret key. The packets carrying correct capability tokens are sent to IPRewrite, which sets a packets destination IP to that of the target website and destination port to port 22433. Unprivileged packets follow UDP and ICMP traffic. Both privileged and unprivileged owns are processed by some standard routing elements. Then, privileged packets are queued into a high-priority queue while other packets own into a low-priority queue. A PrioSched element is used to multiplex packets from these two queues to the output network interface card (NIC). PrioSched is a strict priority scheduler, which always tries the high-priority queue first and then the low-priority one, returning the first packet it finds. This ensures that privileged traffic receives service first. Though we explain our implementation here using only two priority classes, the whole architecture can be trivially adapted to accommodate multiple priority classes. To establish a privileged connection, packets from the target web server to a privileged client must bear the fictitious source address and port in that clients privilege URL.

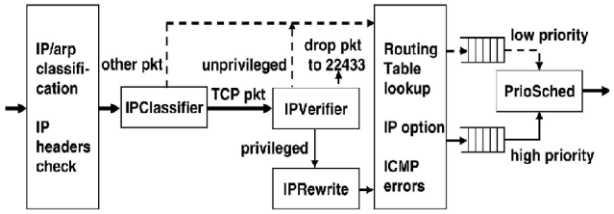

Figure 2 : WRAPS elements on a Click packet forwarding path [8]

3. CONCLUSION

The literature survey presents existing mitigation and prevention techniques for DDoS attacks. Depends on the Mitigation of DDoS attack on web services, Web Referral Architecture for Privileged Services (WRAPS) survey has noted that researchers attempt to detect DDoS attacks from three different layers: IP layer, TCP layer, and application layer. WRAPS does not require installing anything on a web client, but it need to edge routers for the deployment of the protocol. One of the limitations, that the discovery of referrer website is not transparent to clients, could be overcome by using the technique similar to Dynamic DNS to allow a target website to dynamically map it's domain name to its referrer site's IP address when it is undergoing a DDoS attack. The future work is mainly concentrated to overcome this limitation by the above method and also by using the client's ISP (Internet Service Provider) be its referrer.

4. REFERENCES

[1] W. J. Blackert, D. M. Gregg, A. K. Castner, E. M. Kyle, R. L. Hom, R. M. Jokerst, "Analyzing Interaction Between Distributed Denial of Service Attacks And Mitigation Technologies". 0-7695-1897-4/03/2003 IEEE.

[2] Abraham Yaar, Adrian Perrig and Dawn Song, "Pi: A Path Identi cation Mechanism to Defend against DDoS Attacks". Proceedings of the 2003 IEEE Symposium on Security and Privacy, (SP.03).

[3] Cheol-Joo Chae, Seoung-Hyeon Lee, Jae-Seung Lee and Jae-Kwang Lee , "A Study of Defense DDoS Attacks using IP Traceback International Conference on Intelligent Pervasive Computing". IEEE 2007.

[4] Zhenhai Duan, Xin Yuan, Jaideep Chandrashekar, "Controlling IP Spooing through Interdomain Packet Filters". IEEE Transactions on dependable and secure computing, vol. 5, no. 1, January-March 2008.

[5] Vrizlynn L. L. Thing, Morris Sloman and Naranker Dulay, "Adaptive Response System for Distributed Denial-of Service Attacks". Institute for Infocom Research and Imperial College London PhD Thesis, 2008.

[6] M.Nagaratna, Dr. V.Kamakshi Prasad and S.Tanuz Kumar, "Detecting and Preventing IP-spoofed DDoS Attacks by Encrypted Marking based Detection And Filtering (EMDAF)". International Conference on Advances in Recent Technologies in Communication and Computing, IEEE 2009.

[7] Suriadi Suriadi, Andrew Clark and Desmond Schmidt, "Validating Denial of Service Vulnerabilities in Web Services". Fourth International Conference on Network and System Security, IEEE 2010

[8] XiaoFeng Wang and Michael K. Reiter, "Using Web-Referral Architectures to Mitigate Denial-of-Service Threats". IEEE Transactions on dependable and secure computing, vol. 7, no. 2, April-June 2010.