ISSN:0975-9646

Denial of Service Mitigation Method

Madhuri H. Bhagwat, Amol P. Pande

Department of Computer Engineering,
Datta Meghe College of Engineering, Airoli, Maharashtra

***Abstract*— The Denial of service and distributed denial of service are the major threats faced today by most websites. By detecting and mitigating this threat is difficult. The paper reviews the proposed work on one method to mitigate this threat is use of web referral architecture for privileged service (WRAPS). Using the website graph structure a new web referral architecture for privileged service ("WRAPS") is proposed by authors[1]. WRAPS allows a legitimate client to obtain a privilege URL through a simple click on a referral hyperlink, from a website trusted by the target website. Using that URL, the client can get privileged access to the target website in a manner that is far less vulnerable to a distributed denial-of-service (DDoS) flooding attack than normal access would be. WRAPS does not require changes to web client software and is extremely lightweight for referrer websites, which makes its deployment easy. There are some limitations over the web referral architecture for privileged service that is, it uses only static addresses and also domain name system is not resolved because the privilege user uses the privilege URL to access the target web site. This can be overcome by using dynamic IP address in subnet gives high flexibility to this system and using Dynamic DNS by just installing the dynamic DNS software at the referral website , it maps the domain name of target website to IP address of privileged user.**

***Index Terms*—Denial of Service, WRAPS, Website Graph.**

1. INTRODUCTION

Denial of service attack is the major attack in today's Internet world. In 2000 major websites crashes due to the distributed denial of service attack for example, Yahoo!, CNN.com, Amazon.com.

Denial of service attack is the type of attack in which attacker prevents legitimate clients to access service from using desired resources. There are various types of denial of service attack. Here is the description of the some of major attacks related to our paper is:

1. Vulnerability-based and Flooding Attacks: The different types of denial of service attacks can be broadly classified into vulnerability attacks (also called semantic attacks) and flooding attacks (also called brute-force attacks). A DoS vulnerability attack exploits one or more flaws in a policy or in the mechanism that enforces the policy, or a bug in the software that implements the target system, and aims to consume excessive amount of resources of the target by sending it a few carefully crafted requests. For example, in the Ping-of-Death (POD) attack, an attacker cause certain operating systems to crash or reboot by sending a fragmented oversized ICMP (Internet Control Message Protocol) datagrams [CERT/CC 1996a]. A DoS brute-force attack, on the other hand, aims to deny service to legitimate users of a service by invoking vast amount of seemingly valid service requests and trying to exhaust a key resource of the target. For example, in a User Datagram Protocol (UDP) flood attack, an attacker sends excessively high number of UDP segments to random ports on a target host to saturate its bandwidth, rendering the target unreachable by other hosts [CERT/CC 1996c].
2. SYN flood attack [7]: It is also known as the Transmission Control Protocol (TCP) SYN attack, and is based on exploiting the standard TCP three-way handshake. The TCP three-way handshake requires a three-packet exchange to be performed before a client can officially use the service. A server, upon receiving an initial SYN (synchronize/start) request from a client, sends back a SYN/ACK (synchronize/acknowledge) packet and waits for the client to send the final ACK (acknowledge). However, it is possible to send a barrage of initial SYN's without sending the corresponding ACK's, essentially leaving the server waiting for the non-existent ACK's [5]. Considering that the server only has a limited buffer queue for new connections, SYN Flood results in the server being unable to process other incoming connections as the queue gets overloaded [6].
3. UDP Flood attack [7]: It is based on UDP echo and character generator services provided by most computers on a network. The attacker uses forged UDP packets to connect the echo service on one machine to the character generator (chargen) service on another machine. The result is that the two services consume all available network bandwidth between the machines as they exchange characters between themselves. A variation of this attack called ICMP Flood, floods a machine with ICMP packets instead of UDP packets.

Distributed Denial of Service attack (DDoS) [8] 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.

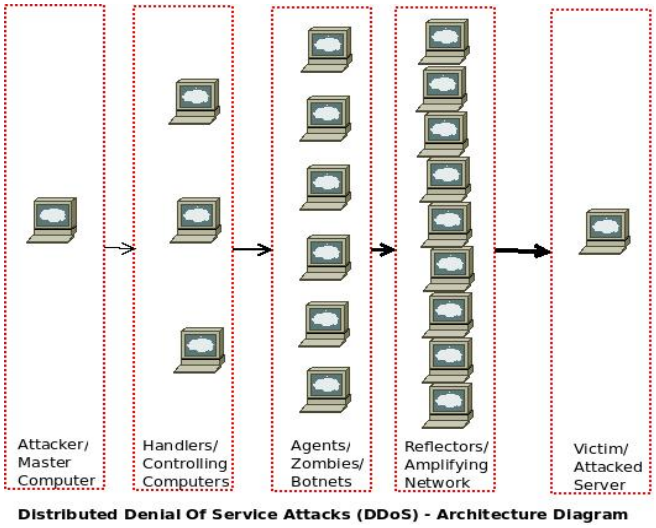

Fig. 1 Architecture diagram of DDoS.

As shown in fig 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.

In this paper there is a solution for the denial of service attack and distributed denial of service flood attack which is faced by today's websites and proposing a solution that is web referral architecture based on website graph [9] structure. XiaoFeng Wang and Michael K. Reiter [1] proposed this WRAPS architecture. They proposed that using the website graph structure to mitigate flooding attacks on a website, using new web referral architecture for privileged service *("WRAPS").* WRAPS allows a legitimate client to obtain a privilege URL through a click on a referral hyperlink, from a website trusted by the target website. Using that URL, the client can get privileged access to the target website in a manner that is far less vulnerable to a DDoS flooding attack. WRAPS does not require changes to web client software and is extremely lightweight for referrer websites, which eases its deployment.

To overcome some of the limitations of WRAPS, I tried to give the best solution.

II. LITERATURE SURVEY

In that paper they compared the web referral architecture with that of existing system that is overlay based approach [3] and capability based approach [4] with the WRAP architecture. They show that WRAPS asks only referral websites to offer a lightweight referral service which allows WRAPS to hold the existing referral relationships on the web to protect important websites. WRAPS does not change protocols, routing paths. In wraps there is no need to change client side software. WRAPS uses the capability token to admit the traffic. It distributes capabilities over the network.

XiaoFeng Wang and Michael K. Reiter[1] proposed the WRAPS architecture in the paper , "Using Web- Referral Architectures to Mitigate Denial-of-Service Threats". In this paper they use the implementation method as 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.

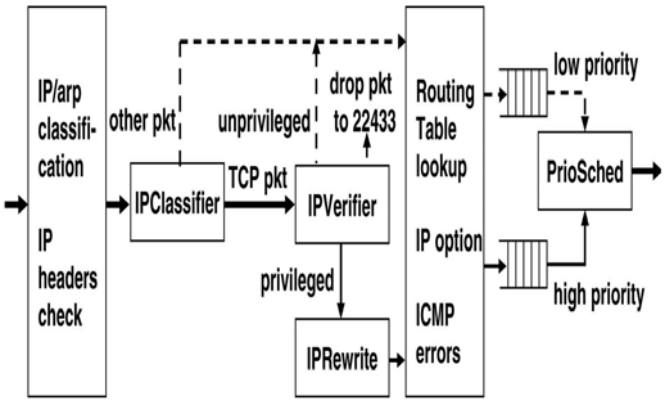

Fig. 2 WRAPS elements on a Click packet forwarding path.

III. CONCLUSION

Web referral architecture uses the privilege URL, protection mechanisms and referral protocol concepts in their proposed system. There are some limitations as mentioned below for using this architecture that mostly arising from the fact that it encodes privilege URLs as IP addresses instead of as domain names.

1. WRAPS supports only clients that use fixed (or infrequently changed) IP addresses.
   To overcome this limitation, using dynamic address in subnet mask in class C networks works as follows:
   In assigning IP addresses to machines, we have two choices. We can either go around typing in the individual address on each machine or we can setup one machine to assign IP addresses to the others.
   The second one called dynamic addressing is preferred for three reasons.
   First, it makes the job of administering the network such as adding new clients, avoiding IP clashes, etc a lot easier. And second, since only those machines that are switched on will need an IP address, we could potentially have more machines on our network with dynamic addressing, than we could with static addressing. Finally, mobile computing has become an everyday reality, and notebook computers have a likelihood of moving from one network to another or from one subnet to another. In such a situation, if we have static IP addressing, we have to reconfigure the machine every time we move it something that is eminently avoidable.
   We do dynamic addressing with DHCP (Dynamic Host Configuration Protocol). To make DHCP work on our network we have to set up a DHCP server.
   In our method we use the dynamic addressing instead of static addressing. WRAPS that supports dynamic NAT users is to generate the client's capability using the client's IP prefix, instead of its whole IP address. This extends privileged service to clients using dynamic addresses in a subnet.
   A subnet is a logical grouping of connected network devices. Nodes on a subnet tend to be located in close physical proximity to each other on a LAN. Network designers employ subnets as a way to partition networks into logical segments for greater ease of administration. When subnets are properly implemented, both the performance and security of networks can be improved.
   For example, if we are using class c network over here. The subnet mask of 255.255.255.0 indicates that this subnet work can contain 256 IP devices.
   So in WRAPS, as the IP address is of 32 bits long and subnet mask for class c network become 24 bits. So there is need to check only 24 bits of the IP address. This gives the WRAPS more flexible, and speed is also more to check whether the user is privileged user or unprivileged user.

2. A user must access the target site using its privileged URL, if she wants privileged service. That is, the domain name of the server cannot be resolved via DNS, and moreover the user must save (e.g., bookmark) her privilege URL from the server when it is updated at the end of a privilege period. In these ways, WRAPS is not transparent to users, and would require client-side modifications to make it transparent.

To overcome this limitation we can use dynamic Domain Name System.
DDNS (Dynamic DNS) [2] is a service that maps Internet domain names to IP addresses. DDNS serves a similar purpose to DNS: DDNS allows anyone hosting a Web or FTP server to advertise a public name to prospective users. Unlike DNS that only works with static IP addresses, DDNS is designed to also support dynamic IP addresses, such as those assigned by a DHCP server. That makes DDNS a good fit for home networks, which often receive dynamic public IP addresses from their Internet provider that occasionally change. To use DDNS, one simply signs up with a DDNS provider and installs network software on their host to monitor its IP address.
For example, dyndns.com provides a free dynamic DDNS service via software that can run on Windows, Mac or

Linux computers. Compared to ordinary DNS, the disadvantage of DDNS is that additional host software, a new potential failure point on the network, must be maintained.

In WRAPS the after confirming that the user is privileged user. Then the referral web site sends the privilege URL. In that the capability token is embedded inside the IP address and port number fields. By using dynamic DNS to allow a target website to dynamically map its domain name to its referrer sites' IP addresses when it is undergoing a DoS attack. The target web site chooses its best shortest path to map dynamic DNS to its referrer sites IP address. There is a need to install the software of dynamic DNS to the referral web site so it can dynamically map the the domain name of the target web site to privileged URL's IP addresses of the privileged users.

REFERENCES

[1] 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.

[2] DDNS - Dynamic DNS By Bradley Mitchell, http://compnetworking.about.com/cs/domainnamesystem/g/bldef_ddns.htm

[3] D. Andersen. Mayday: Distributed filtering for internet services. In *Proceeding of USITS*, 2003.

[4] T. Anderson, T. Roscoe, and D.Wetherall. Preventing internet denialof- service with capabilities. In *Proceedings of Workshop on Hot Topics in Networks (HotNets-II)*, November 2003.

[5] S. Bellovin, "Security problems in the TCPIIP protocol suite,"*Comput. Commun. Rev.***,** vol. 19, no. **2,** pp. 32-48, Apr. 1989.

[6] Cisco Systems, Inc., "Defining strategies to protect against TCP SYN denial of sarvice attacks," July 1999, http://www.cisco.com/warp/public/707/h4tm. l.

[7] Distributed Denial of Service Attacks Lau F., Robin S. H.,Smith M. H.;Trajkovic, L.Systems, Man and Cybermetics, 2000 IEEE International Conference on Volume:3

[8] Abhilash C. S. Student M-Tech Computer science and Engineering, MES College of Engineering, Kuttipuram. And Sunil kumar P. V. and Assistant Professor Department of Computer science and Engineering MES College of Engineering, Kuttipuram, "Mitigation of Distributed Denial of Service (DDoS) Threats".

[9] J. Wu and K. Aberer, "Using Siterank for p2p Web Retrieval," Technical Report IC/2004/31, Swiss Fed. Inst. Technology, Mar. 2004.