Depth-in-Defense Approach against DDoS

Rabia Sirhindi, Asma Basharat and Ahmad Raza Cheema
Information Security Department, College of Signals
National University of Sciences and Technology
Tamiz-ud-din Road Rawalpindi Cantt
Pakistan

Abstract: Distributed denial-of-service attacks (DDoS) impose a great threat to the availability of resources. Not only is the attack difficult to carryout but also the methods and techniques used to prevent these attacks are so complex that it makes the job to protect the resources even harder. An analysis is carried out for various approaches of detection and prevention systems that can be deployed to reduce the effect of the attacks on the victim. In this paper a comparative analysis has been carried out amongst different techniques for prevention against DDoS attacks and at the end a novel solution is proposed.

Keywords: DDoS, DNS, Reflector attack, ACL, SYN-ACK, Filtering.

1. INTRODUCTION

A Denial of Service (DoS) attack is an attempt by the attacker to prevent legitimate users from accessing a service by exhausting the system and network resources with high volumes of useless traffic [17].

According to the Computer Incident Advisory Capability (CIAC), the first DDoS attacks occurred in the summer of 1999 [2]. In February 2000, one of the first major DDoS attacks was instigated against Yahoo.com which kept it off the Internet for about 2 hours and cost a major loss in advertising revenue [3]. Another DDoS attack occurred on October 20, 2002 against the 13 root servers that provide the Domain Name System (DNS) service to Internet users around the world. Although the attack only lasted for an hour and the effects were hardly noticeable to the average Internet user, it caused 7 of the 13 root servers to shut down, demonstrating the vulnerability of the Internet to DDoS attacks [4].

Distributed denial-of-service (DDoS) attack is more powerful DoS attack using a number of sources to attack a victim. It amplifies the DoS attack effect by compromising a group of hosts that are in turn used to attack some victim host in unison. These compromised hosts are distinguished as masters and salves. Each master controls a number of slaves. The masters take a single command from the attacker and instruct the slaves (zombies) who actually generate huge volumes of traffic towards the victim causing a

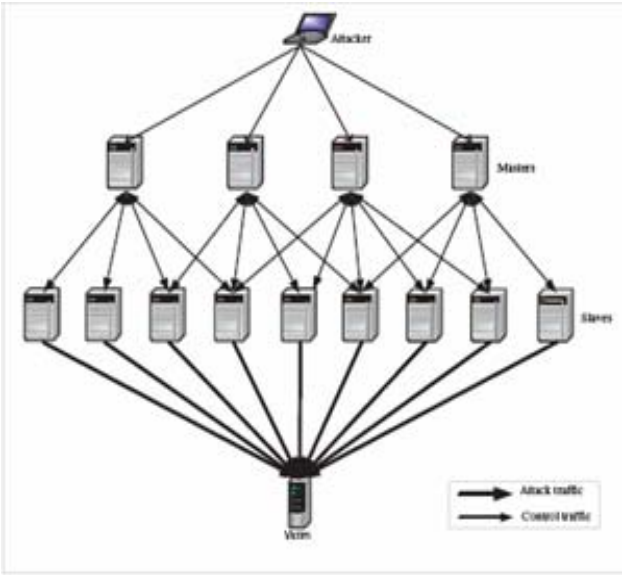

Fig.1. DDoS architecture

DoS attack to occur. This indirect attack technique makes discovery of the attacker very difficult.

There are more than single targets in a DDoS attack. Victims can be identified as either ‘primary’ whose services are directly under attack, or ‘secondary’ that are used as intermediary systems to launch an attack such as masters and slaves. The use of secondary victims in a DDoS attack provides the attacker with the ability to

wage a much larger and more disruptive attack while remaining anonymous since the secondary victims actually perform the attack making it more difficult for network forensics to track down the real attacker [1].

In order to facilitate DDoS attacks, the attackers need to have several hundred to several thousand compromised hosts. The first step in launching DDoS attack is to find weakly secured systems that can be compromised due to vulnerabilities in standard network service programs and common weak configurations in operating systems. Once the system is broken into, some software is installed on it to conceal the break-in and hide subsequent attacker activity. A special process is then installed to remotely control the compromised machine. This process accepts commands over the Internet and in response launches an attack against some designated victim. The address of the machine that is taken over is noted. All these steps are highly automated. Finally at the time of an attack the attacker runs a single command issued to the master (handler) which in turn sends command packets to all the captured machines (zombies or slaves) instructing them to launch a particular attack against a specific victim. A DDoS attack and its components are shown in the Fig.1.

This paper presents an overview of the DDoS attacks and preventive techniques that can be used to overcome the effects of these attacks. Section 2 provides a categorization of DDoS attacks and their problems. Section 3 explores various defensive approaches relating to detection, prevention and response to such attacks. In section 4 we present a comprehensive DDoS defense mechanism.

2. TYPES OF DDOS ATTACKS

DDoS flooding attacks can be broadly classified into two categories: direct attacks and reflector attacks [10]. Direct attacks are launched by the attacker directly sending TCP, UDP or ICMP packets to the victim as described above. A reflector attack is an indirect attack in which intermediary nodes are used to launch attack. A reflector is, any host that sends a response packet if it receives a request packet. Request packets using spoofed address of the victim are continuously sent to a reflector which in turn will reply as if the request had been originated by the victim.

2.1 DNS Reflector Attacks

One of the recent reflector attacks involve the use of DNS servers. DNS servers offer two possibilities for reflection. The first is a reflector simply sending a DNS reply in response to a spoofed DNS request. The second form of DNS reflection concerns DNS servers that in turn recursively query other servers to resolve a request. When recursive queries from any client are processed by the server it is called an *open recursive server*. If the victim is an open recursive name server for a particular zone, then the attacker can issue a stream of queries to a large number of name servers that will in turn cause those name servers to bombard the victim server with recursive queries.

2.2 TCP Reflector Attacks

In TCP-based reflector DDoS attack, the attacker sends SYN packets to many reflectors. Each corresponding SYN-ACK packet is then sent to the victim [6]. Attack amplification is achieved through the multiple retransmissions of SYN-ACK packets after each time out. DDoS attacks can also be classified as bandwidth depletion and resource depletion attacks [5]. Bandwidth depletion attacks target the victim network where network resources (such as bandwidth, router buffers, etc) are exhausted by flooding it with unwanted traffic so that legitimate traffic is unable to reach the victim. Resource depletion attacks tie-up the resources of the victim system (such as memory, processing power, etc) so that legitimate users are denied of service.

Fig.2. DDoS reflector attack

3. DDoS DEFENSES

There are various approaches of defenses against DDoS attacks. This section covers few of them which are most effective but none of them provides complete protection. Each of them has it own benefits and drawbacks.

3.1 Ingress/Egress Filtering

This efficient preemptive technique takes into account the fact that DDoS attacks often use spoofed IP addresses. Ingress and egress filtering enable routers to discard any traffic that uses illegitimate IP addresses [8]. The effectiveness of filtering increases as we move farther from the victim toward the source of attack.

3.2 IP Hopping

IP hopping or moving the target defense is a method in which the system frequently changes its IP address when an attack is detected. When the IP is changed the edge routers will drop all the attack packets. However, this change in IP address needs to be reflected in DNS Name Server entries and routing table entries so that legitimate packets can reach the host. Moreover DNS tracing functions can be used to target the new IP address.

3.3 Client Puzzles

Client puzzles are required to hinder the ability and speed of the attacking zombies [16]. The attacking hosts are required to correctly solve a small puzzle or answer some random question before establishing a connection, therefore creating bottleneck processes on the zombie.

3.4 Traceback Techniques

Traceback techniques are response mechanisms used to trace the path traversed by the attack packets [9][14]. Once an attack is detected the victim can trace back to the zombies and stop the attack. However trace back technique fail in the DDoS reflector attacks where the attacking systems are legitimate hosts responding to bogus spoofed traffic.

3.5 Pushback

Pushback is a router-based detection and response technique in which the router classifies the traffic according to a common feature into aggregates [13]. The routers use Aggregate-based Congestion Control (ACC) to identify the illegitimate traffic. The router then sends a pushback request to the upstream routers to rate limit the aggregates. This approach iteratively blocks attacking network segments.

3.6 Capability Based Approach

Capability based approach is used to block attack packets close to source. The receiving system can specify the type of traffic that should be forwarded to it. Routers forward only request packets and packets with capabilities [11].

3.7 Load Balancing

This is a DDoS tolerant approach in which the critical network resources and services are replicated. Thus improving the quality of services and mitigating the DDoS attack effect.

4. PROPOSED SOLUTION

We present a comprehensive solution for defense against DDoS attacks. A comprehensive solution can be deployed in three phases. The first phase involves preemption and prevention (before the attack). The second phase includes detection, filtering and mitigation of the attack (during the attack). The final phase is the recovery and traceback to the source of attack (after the attack).

The most effective method to counter DDoS is to stop it near the source of the attack, to prevent its effects from spreading further into the network. This line of defense is efficiently implemented at the routers that monitor the network traffic and filter it according to a set of configured rules. The most appropriate location for the deployment of such filters is the gateway routers of the networks that have the potential to become zombies or slaves. Therefore for the first line of defense we have selected Ingress/Egress filtering that will block and discard any spoofed attack packets [8]. This approach is simple, efficient and easy to implement. This should be widely deployed over the Internet. The routers are also configured using Access-Control List (ACL) to block external broadcasts to prevent internal hosts from becoming reflectors.

The second line of defense is the deployment of indirection networks or overlay-based protection which acts as first-level firewall [12]. It distinguishes between legitimate and unauthorized traffic. All overlay nodes are publicly known but the identity of the forwarding overlay node is surreptitious. The user communicates with the protected system through the secret forwarding

overlay nodes. The forwarding overlay node is randomly chosen and regularly changed. However if the attacker discovers the real time pattern of the selection of the overlay node through which the client is routing traffic then the scheme become susceptible to attack. Therefore to minimize this impact we propose the implementation of a proxy or Prolexic that accepts connection requests (SYN packets). Normal SYN/ACK replies are sent back to the client. Only if the client sends the final ACK of the three-way handshake, its connection is established with the protected host. Prolexic is especially designed to protect against SYN flooding which can bypass a compromised overlay node. Moreover to prevent automated flooding attacks, Graphic Turing tests or CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) are implemented on the Prolexic.

The third and final line of defense proposed for the mitigation of the DDoS attack is implemented at the potential victim system. If an attack is detected at the victim, the victim will accept connections from only those clients that can correctly solve a client puzzle or pass a turing test to validate their authenticity.

Implementing various defense mechanisms on different levels provide defense in-depth making it difficult to carry out a DDoS attack. The solution we have proposed will mitigate the effect of the DDoS attack, block protocol design exploits, prevent and detect automated attacks and create process bottlenecks for the intermediary attack agents.

5. CONCLUSION

In this paper we focused on the classification of DDoS attack and defense methods. We have presented a potential solution that aims to prevent the attack and mitigating its effects if it occurs. The solution involves the configuration of internet-wide ingress filtering rules at the border routers to prevent spoofed attacks. This technique prevents the creation of a master-slave DDoS network. Another level of security is added by the implementation of overlay networks that provide indirection and mitigation to the attack. A prolexic is used to block automated traffic and filter out legitimate connections. Turing tests and client puzzles are used as the last layer of defense that creates bottlenecks in the zombie network.

6. FUTURE WORK

We are working on an algorithm based on the current research and to test this approach in real network other than simulation to get the actual performance analysis of this solution for DDoS.

7. ACKNOWLEDGMENT

We would like to thank Mr. Imtiaz A. Khokhar for providing us with resources and giving us confidence to complete this paper.

References:

[1] Stephen M. Specht and Ruby B. Lee. *Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures*. *Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems*, 2004 International Workshop on security in Parallel and Distributed Systems, September 2004.

[2] Paul J. Criscuolo. *Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000, And Stacheldraht CIAC-2319*. Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.

[3] "Yahoo on Trail of Site Hackers", *Wired.com, February 8, 2000.* http://www.wired.com/news/ business/ 0,1367,34221,00.html (15 May 2003).

[4] "Powerful Attack Cripples Internet". *Associated Press for Fox News* 23 October 2002. http://www.foxnews.com/story/0,2933,66438,00.html. (9 April 2003).

[5] Christos Douligeris, Aikaterini Mitrokotsa. *DDoS Attacks And Defense Mechanisms: A Classification*.

[6] S. Gibson, *Distributed Reflection Denial of Service.* February 22nd, 2002.

[7] Randal Vaughn and Gadi Evron. *DNS Amplification Attacks*. Preliminary release March 17, 2006.

[8] P. Ferguson, D. Senie. *Network Ingress Filtering: Defeating Denial Of Service Attacks Which Employ IP Source Address Spoofing*. RFC2827, Cisco Systems Inc., May 2000.

[9] S. Savage, D.Wetherall, A. Karlin, and T. Anderson. *Practical Network Support for IP Traceback.* In ACM SIGCOMM, August 2000.

[10] Vern Paxson. *An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks*. In Proc.

Computer Communication Review vol. 31(3), July 2001.

[11] Xiaowei Yang, David Wetherall, Thomas Anderson. *A DoS Limiting Network Architecture*. In ACM SIGCOMM Philadelphia, August 2005.

[12] A. D. Keromytis, A. D. Misra, & Rubenstein, D. *SOS: An Architecture for Mitigating DDoS Attacks*. IEEE Journal on Selected Areas of Communications (JSAC) January 2004.

[13] J. Ioannidis, S. M. Bellovin. *Implementing Pushback Router-Based Defense against DDoS Attacks.* Inn Proc. IEEE INFOCOMM Anchorage, AK, USA. April 2001.

[14] S. M. Bellovin. *ICMP Traceback Messages*. Work in Progress, Internet Draft draft-bellovin-itrace-00.txt, March 2000.

[15] Yacine Bouzida et al. *Detecting and Reacting against Distributed Denial of Service Attacks*. IEEE ICC 2006. (diagram reference)

[16] Timothy John McNevin. *Mitigating Network-Based Denial-Of-Service Attacks With Client Puzzles*. Virginia Polytechnic Institute and State University April 15, 2005

[17] http://www.cert.org/tech_tips/denial_of_service.html BackOrifice, CERT Vulnerability Note VN-98.07, Friday, October 1998 http://www.cert.org/vul_notes/VN-98.07.backorifice.html