Journal of Information and Operations Management
ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-29-33
Available online at http://www.bioinfo.in/contents.php?id=55

A COMPREHENSIVE STUDY OF DDOS ATTACKS AND DEFENSE MECHANISMS

SHUCHI JUYAL[1] AND RADHIKA PRABHAKAR[2]

Department of Computer Application, Graphic Era University, Dehradun, India
*Corresponding Auther: Email– [1]shuchi.juyalb@gmail.com, [2]radhikadun@gmail.com

Received: December 12, 2011; Accepted: January 15, 2012

Abstract- Distributed Denial of Service (DDoS) attacks on network systems in the Internet have become highly significant incidents and required to be solved immediately. These attacks are very complex and aim at crippling applications, servers, and whole networks, and disrupting legitimate user's communication. Various schemes have been proposed to provide defensive measures against these attacks, but still an efficient defensive approach is yet to come. The main idea of this paper is to presents basics of DDoS attacks, their classifications and classification of existing mechanisms to handle them. This offers future research scope to defend against DDoS attacks and handle them in an efficient way.
Keywords - DoS, DDoS, Network Security, Defense, Zombie.

Citation: Shuchi Juyal and Radhika Prabhakar (2012) A Comprehensive Study of Ddos Attacks and Defense Mechanisms. Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-29-33.

Introduction

Today, Internet is used in our everyday lives to perform different tasks. Even most of the traditional services, i.e. banking, transportation, education, defense, etc, are automated through Internet. In addition to these lucrative benefits, it is also vulnerable for various threats. Nowadays, one of such attack is denial of service (DoS) attack. It is most serious threat to Internet now. (Definition) The first publicly known DDoS program was developed in 1998 [1]. In November 1999, the Computer Emergency Response Team Coordination Center (CERT/CC) invited 30 experts from around the world to address the DDoS attack problem [2]. Short after, in February, 2000, seven of the Web's busiest sites - Yahoo.com, Buy.com, ZDNet.com, eBay.com, CNN.com, Amazon.com, and Etrade.com were attacked. Each site was overloaded by attack traffic coming from multiple locations, for hours [3]. Nowadays DDoS attacks become more sophisticated and difficult to handle.

Defensive measures are required to detect and recover from these attacks. Most of the defense actions are taken only after the attack is launched. A better approach is to hold back the attack before it harms the victim.

In this paper, we will discuss about basic difference between DoS and DDoS attacks. A DoS attack is launched through a single host whereas a DDoS attack is launched as a coordinated attack through a group of compromised hosts to one or more targets. DDoS attacks are classified based on
deployment ,attack rates, weakness exploited, and attacking methods. Each classification have different types of attacks based on certain common properties.

So, none of them gives a comprehensive solution but deal with a part of the DDoS problem. Moreover these attacks are very dynamic to escape from existing defense systems. So how to defend against DDoS attacks has become one of the extremely important research issues in the Internet community. Here we discuss some of the mechanisms to handle DDoS attacks. We have also presented an overview of the automated tools used to implement DDoS attacks, their effects and impacts.

Rest of the paper is organized as follows: basic overview of the DDoS problem is presented in section II. Section III includes a classification of different DDoS attack mechanisms. Section IV discusses some tools identified to implement DDoS attacks. Section V contains defense mechanisms for various DDoS attacks. Finally, section VI concludes the paper.

DDoS Attack Overview

A Denial of Service (DoS) attack can be characterized as an attack with the purpose of preventing legitimate users from using a victim computing system or network resource [4]. There are four basic elements involved in DDoS Attack-

Attack source: Initiator of the Attack is a machine, handled by attacker.

Masters Agent: control various agents to implement the attack in coordination.

Slave Agents: also known as attack daemons, and are responsible for attacking the victim directly.

Victim: A victim is a target host that is harmed.

Hierarchy of the attack elements is given in fig 1.

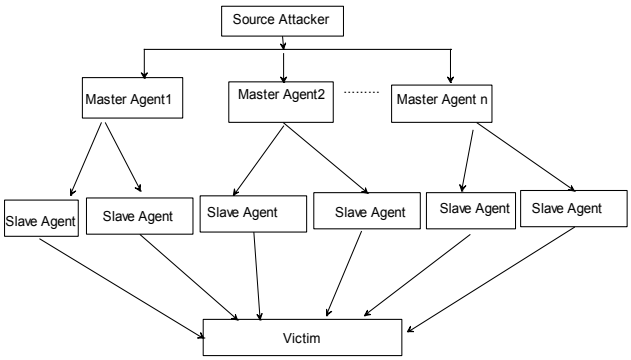

Fig. 1- Elements of DDoS Attack

A Distributed Denial of Service (DDoS) attack is an internet attack that is implemented as a coordinated attack and is launched indirectly through many compromised computers at a large scale. Source attacker uses client-server technology to multiply effectiveness of the Denial of Service significantly by exploiting the resources of multiple ignorant assistant computers.

A DDoS attack is carried out by a group of machines (agents.) sends packets to a victim host on receiving commands from a machine (master.) controlled by the attacker.

DDoS Attack Mechanisms

Wide range of attack mechanisms are used to implement distributed denial of service attacks. This section describes classification of those attack mechanisms which includes their characteristics and effect

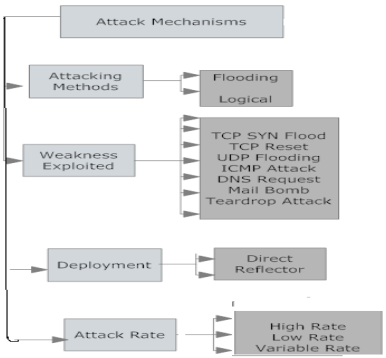

Fig. 2- Attack mechanisms

DDoS Attacks Based on Attack Methods

Flooding Attack

Flooding attack also named as brute force attack is performed using TCP. In flooding DDoS attack, mangled packets that look legitimate and valid are sent to block the computational resources on target victim so that it can not serve its legitimate users. Network bandwidth, disk space, CPU time, data structures, network connections are few of the resources consumed by this attack.

Logical Attack

Logical attacks take advantage of a specific feature or implementation bug of some protocol installed at target victim to consume an excess amount of its resources .For example, in the TCP SYN attack, the exploited feature is the allocation of substantial space in a connection queue immediately upon receipt of a TCP SYN request. The attacker initiates multiple connections that are never completed, thus filling up the connection queue [6].

DDoS Attacks Based on Weakness Exploitation

TCP SYN Flooding

Any system providing TCP-based network services is is vulnerable to this attack. This attack sends a flood of TCP/SYN connection packets with forged sender ip. In response to this request server provides a half-open connection by sending back TCP/SYN-ACK packet and then waits for TCP/ACK packet. But because of the forged sender address, the response never comes. Such half - open connections consume various resources on the server and limits the number of connections on a server. Finally the system crashes (fig 3.a,b).

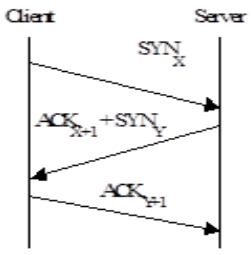

Fig.3a- TCP Synchronization

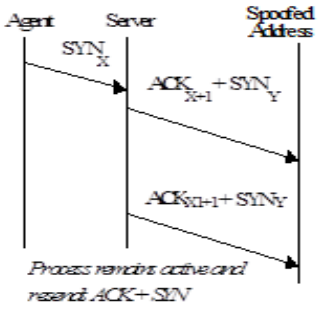

Fig 3b.TCP SYN Attack

ICMP Attack

Also known as Smurf attack sends forged ICMP echo request packets to IP broadcast addresses. A large amount of ICMP echo reply packets are sent via an intermediary site to a victim. This large flow of echo reply causes network congestion and disruption of resources from victim. ICMP datagram use the .ping command to construct oversized ICMP datagram to launch ping attack.

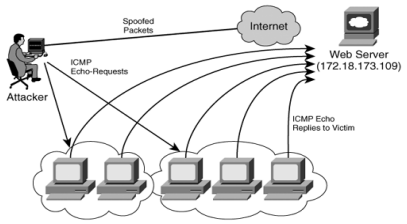

Fig. 4- Smurf attack.

TCP Reset
The main idea behind a TCP reset attack is to falsely terminate an established TCP connection without the consent of the two communicating parties. The attacker sets the RST bit on the spoofed packet, and when this packet is received by a communicating host, it immediately terminates the connection. Attack holds till the connection is reestablished.

UDP Flooding
This kind of attack can not only impair the hosts services, but also congest or slow down the intervening network. In this attack the attacker sends the packet to victim's random port. On receiving this arrived packet, victim system, try to find which application is waiting on that destination port. But actually there is no application waiting on that port. Thus it generates an ICMP response with destination unreachable to forged source address. As large numbers of such UDP packets are received by the victim, it goes down as an infinite loop goes between two UDP services.

Mail Bomb
An email attack, used to consume victim's disk space by sending a massive amount of emails at a time. This attack is also a kind of flood attack.

Teardrop Attack
Reassembly of data packet is a vulnerable point location for teardrop attack. It involves sending invalid or garbage IP fragments with overlapping or oversized, payloads to the target machine and forces them to crash, hang, or reboot .

DNS Request Attack
In this attack, the attacker sends a large number of UDP-based DNS requests to a name server using victim's IP. Then the name server responds by sending back to the victim destination which was spoofed. It causes amplification effect of DNS response, which lead to high bandwidth consumption.

DDoS Attacks Based on Deployment

Direct Attack
This attack is directly applied through zombies by sending large amount of malicious packets to the target machine. To serve this purpose, attackers gained control over thousands or even millions of vulnerable machines and then route the malicious packets from distributed zombies to the victim machine.

Reflector Attack
This attack uses indirect way to send packets to the victim system. The zombies continuously send TCP SYN packets to the normal innocent hosts with the source address spoofed as the address of the victim. These innocent hosts reply with SYN/ACK to the victim. The victim becomes busy in handling these replies and at last crashes or stops working.

DDoS Attacks Based on Attack Rate

High Rate Disruptive
Disruption of Internet services by sending volume of Packets at a point in time from distributed locations results in High Rate Disruptive attack.

Diluted Low Rate Degrading
Zombies are used to send large volume of malicious packets at low rate in a coordinated manner. It's a slow process of degrading network performance.

Varied Rate
It is a combination of high rate disruptive and low rate degrading attacks. It is a complex attack that uses attack tools to generate a mixture of packets at high rates and low rates. These types of attacks are toughest to detect and characterize.

DDoS Attack Tools
It becomes easy to implement DDoS attack as lots of automated tools are now available. To scan and propagate among vulnerable hosts, DDoS attackers install attack tools on the compromised hosts and use them as the attacking machines. Some of the most common tools are:

• **Trinoo** (Mirkovic & Reiher, 2004; Dittrich, 1999) can be used to launch a coordinated UDP flooding attack against target system. Trinoo deploys master/slave architecture in which a source attacker controls a number of Trinoo master machines. The machines can't be taken over by any other machine as both master and slave are password protected.Wintrinoo is a Windows version of trinoo that was first reported to CERT on February 16, 2000.

• **TFN** (Dittrich, 1999) can implement Smurf (Huegen, 2000; Azrina & Othman, n.d.), SYN Flood(Schuba et al., 1997; Farrow, n.d.; CERT Advisory,1996), UDP Flood (Azrina & Othman, n.d.), and ICMP Flood (Azrina & Othman, n.d.; Papadopoulos et al., 2003) attacks. It uses a command line interface via ICMP echo reply packets to communicate between the attack source and the control master program.

• **TFN2K** (Douligeris & Mitrokotsa, 2004; Barlow &Thrower, 2000; CERT Coordination Center, 1999) a more advanced version of TFN network which uses key-based CAST-256 algorithm for encryption between master and slave communication. It uses TCP, UDP, ICMP, or all three for
communication. TFN2K can implement Smurf, SYN, UDP, and ICMP Flood attacks.

• **Shaft** (Dietrich, Long, & Dittrich, 2000) It works like Trinoo but the communication is done through ports. Thus, it has ability to switch control master servers and ports in real time.Communication is achieved using UDP packets. Shaft can implement UDP, ICMP, and TCP flooding attack.

• **Mstream** (Dittrich et al., 2000) It attacks target machine with a TCP ACK flood by using TCP and UDP packet communication. Communication is not encrypted and the master connects via telnet to zombie. Masters can be controlled remotely by one or more attackers using a password protected interactive login.

• **Trinity** (Hancock, 2000; Marchesseau, 2000) is an IRC based DDoS attack tool. It can implement UDP, IP fragment, TCP SYN, TCP RST, TCP ACK, and other flooding attacks. Each trinity compromise machine joins a specified IRC channel and waits for commands. It uses IRC service for communication between attacker and agents.

DDoS Defense Mechanisms
Large numbers of defense methods have been proposed by researchers to struggle DDoS attacks. A detailed description of this classification is given below:

Attack Prevention
Attack Prevention focuses on the strategy to avoid well known DDoS attacks that are launched from edge routers.
Attack prevention schemes of DDoS attacks are signature based and thus unable to handle unknown patches that do not exist in the

database. So these are considered forensic defense methods .So it is required to keep all machines on the Internet up to date with latest security patches. Various prevention techniques are:-

Firewalls

Firewalls can prevent users from launching simple flooding type attacks at IP level. Firewalls have simple rules based on which system can allow or deny protocols, ports, or IP addresses. However, some complex attacks (eg.on port 80) can't be handled as firewall is unable to distinguish good traffic from DDoS attack traffic.

Install Latest Security Patches

Latest security packets are needed to be installed and updated so as their signatures are verified in target systems. It removes known security holes by installing all relevant latest security patches and prevents re-exploitation of vulnerabilities

IP hopping

It aims to solve IP spoofing, a fundamental weakness of the Internet. Its basic idea is to change the victim's IP address with a prespecified set of IP address ranges, thereby invalidating the old address. But the computer is still vulnerable because the attack can be launched at the new IP address.

Since the communication between attackers and "zombies" is encrypted, only "zombies" can be exposed instead of attackers. According to the Internet Architecture

Working Group (2005), the percentage of spoofed attacks is declining.Only 4 out of 1127 customer impacting DDoS attacks on a large network used spoofed sources in 2004 [6].

Remove unused services

Only the necessary services should be open because less is the number of services lower will be the vulnerability at target. Default installations of operating systems often include many applications that may not needed by a user, so one should delete them.

DDoS Attack Detection

Attack detection aims to detect an ongoing attack as soon as possible without affecting the legitimate traffic. It detects the attack based on timing and activity. The classification is as follows:-

Timing based detection

These detection techniques classify the attacks detection by the timing of their occurrence.

Passive detection

Which means the defense actions are taken only after the DDoS attacks are launched. Here the target host or network is harmed before the attack source(s) can be found and controlled.

On-time detection

It detects the attack at the time it is going.

Proactive detection

It detects the attack before it actually harms the victim or network.

Activity based detection

These detection techniques classify the attacks detection based on the behaviors and signatures.

Pattern or signature based attack detection

This approach requires a priori knowledge of attack signatures. The knowledge of the signature comes from the security experts who manually analyze previous attack patterns .Finally the incoming traffic is matched against this knowledge base to identify intrusion.

Anomaly based attack detection

Anomaly based detection analyze previous profiles of the inco ing packets to detect novel attacks. It detects an intrusion by finding deviations from that normal behavior.

The biggest problem is that it is difficult to generate normal traffic profiles due to which it false positive generate provide more accurate normal profiles. But it increases the computational overhead.

Hybrid attack detection

It is a combination of signature and anomaly based detection. This approach decreases the number of false positives .On the other hand it increases complexity and implementation cost .

Third party detection

In this defense mechanism, target system itself will not detect the attack but recruits a third party to do this.

DDoS Attack Response

In includes the actions taken after the attack is launched. It can't stop the victim to get harmed but try to minimize the effects.

Attack source identification

In this mechanism one has to stop the attack traffic at the source itself. But it is very difficult to track IP traffic as it runs through the IP protocol which is stateless and also the source address is spoofed .To overcome this limitation, several technical supports have been proposed which supports IP traceability.

Filtering

It involves filtering out of malicious packets from legitimate packets. As it is difficult to distinguish a malicious packet this technique cause a large number of false positives.

Rate-limiting

It limits the number of packets coming in attack traffic if attack is detected. Less number of packets means less harm to victim

Reconfiguration

Reconfiguration means to change the victim location geographically either by changing its topology or by isolating the attack machines.

DDoS Attack Tolerance and Mitigation

This mechanism works on the assumption that it is impossible to prevent or stop DDoS completely. Thus it focuses on victim's level of tolerance and quality of service as the attack goes on. This is not a comprehensive solution but will help a victim to serve its legitimate users.

Over provisioning.

Additional resources like pool of servers with load balancer, high bandwidth link between victim machine, and upstream routers are added to victim who provides support to tolerate these attacks.

Router's Queue Management

In this mechanism router queue is unfair between the traffic flows, thus reducing congestion.

Router's Traffic Scheduling

It applies costly delays and state monitoring algorithms to provide routing between different traffic flows so as to control congestion.

Target Roaming

Random location change by the active servers within distributed homogeneous servers proactively helps to tolerate DDoS attacks impact.

Conclusion

DDoS attacks are quite advanced methods of attacking a network system to make it unusable to legitimate network users. A number

of automated tools are used to launch these attacks. In this paper, we tried to scope the DDoS problem, different classes of DDoS attacks and current defense mechanisms. This provides better understanding of the problem. The current defense mechanisms discussed in this paper are somehow far from protecting the Internet from DDoS attacks.

For the DDoS attacks, what is desirable is a more comprehensive solution that can defend against both known attacks and new variants of DDoS attacks and attack tools. This may help in facilitating research into more comprehensive, multi-tiered solutions, rather than just designing specific countermeasures for a specific attack.

Acknowledgment

I gratefully acknowledge Mr. B.B. Gupta, Department of Computer Science and Engineering, Graphic Era University, Dehradun for his valuable guidance and support throughout the paper.

References

[1] David Dittrich (2000) *A Brief History of DoS.*

[2] Computer Emergency Response Team (1999) *Results of the Distributed-Systems Intruder Workshop*.

[3] CNN.com (2000) *The denial-of-service aftermath.*

[4] David Karig and Ruby Lee (2001) *Princeton University Department of Electrical Engineering Technical Report* CE-L2001-002.

[5] Yang Xiang, Wanlei Zhou and Morshed Chowdhury *School of Information Technology Deakin University Melbourne Campus, Burwood 3125.*

[6] Gupta B.B., Joshi R.C., and Manoj Misra (2009) *Information Security Journal: A Global Perspective.*