ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

A Survey on Latest DoS Attacks:Classification and Defense Mechanisms

Rajkumar[1], ManishaJitendra Nene[2]

Department of Computer Engineering, Defense Institute Of Advanced Technology, Pune, India

Abstract: Distributed Denial of Service (DDoS) is defined as an attack in which mutiple compromised systems are made to attack a single target to make the services unavailable foe legitimate users.It is an attack designed to render a computer or network incapable of providing normal services. DDoS attack uses many compromised intermediate systems, known as *botnets* which are remotely controlled by an attacker to launch these attacks. DDOS attack basically results in the situation where an entity cannot perform an action for which it is authenticated. This usually means that a legitimate node on the network is unable to reach another node or their performance is degraded.
The high interruption and severance caused by DDoS is really posing an immense threat to entire internet world today. Any compromiseto computing, communication and server resources such as sockets, CPU, memory, disk/database bandwidth, I/O bandwidth, router processing etc. for collaborative environment would surely endanger the entire application. It becomes necessary for researchers and developers to understand behaviour of DDoSattack because it affects the target network with little or no advance warning. Hence developing advanced intrusion detection and prevention systems for preventing, detecting, and responding to DDOS attack is a critical need for cyber space.
Our rigorous survey study presented in this paper describes a platform for the study of evolution of DDoS attacks and their defense mechanisms.

Keywords: DDoS, Bots, Malware, IRC.

I. INTRODUCTION

The DDoS attacks are not new to the world of cyber security [1], [2] however the mode of DDOS attacks is changing parallely with the advancement in security solutions. The first documented DDOS attack was reported in August 1999 against a university [3] which lasted for 2 days. On Monday, 7 February 2000 a high-profile DDoS attacks hit Yahoo, the most popular site on the Web which leads to high revenue losses to Yahoo [4]. In October 2002, 9 of the 13 root servers that provide the Domain Name System (DNS) service to Internet users around the world shut down for an hour because of a DDoS flooding attack [5]. Most recently, since September 2012, online banking sites of 9 major U.S. banks e.g. Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T, and HSBC have been continuously the targets of series of powerful DDOS flooding attacks launched by a foreign hacktivist group called ”Izz ad-Din al-Qassam Cyber Fighters” [6]. Reference [7] shows that 46.5% of attacks crosses 1Gbps in 2013 with a jump of 13.5% from 2012.

The Biggest DDoS attack ever was against Spamhaus which reached a peak of 300gbps forcing Spamhaus to move to hosting and service provider CloudFlare [8]. (DDoS), is a relatively simple, yet very powerful technique to attack Internet resources and what makes it more powerful is that detecting the attack is challenging issue because of its legitimate behavior.

Intentions behind the DDoS attack can be any of the following:

A. Revenge

It is perhaps the most common reason for DDOS attack. Current and ex-employees, unsatisfied customers or anyone with a dispute may have motive for attack. Hackers sometimes attack over minor disagreements.

B. Cloaking Criminal Activity

One may use DDoS as a diversion to mask other illegal activities.

C. War

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

In place of physical war, governments are now developing capabilities of cyber war where DDoS can be used as a weapon.

D. Politics

DDoS may be used by political groups and terroriststo digitally silence political opposition.

E. Intellectual challenge

Young enthusiasts who want to show off their capabilities can launch DoS attack.

The rest of the paper is organized as follows:

In section II, the survey study will focus on some categorized attack vectors that leads to DDoS attack. Section III will elaborate some existing DDoS attack strategies and describe several phases ofDDoS attack. Section IVwill categorize different DDoS attacks on the basis of methodology of communication, exploits, spreading techniques and degree of automation. Section V will focus on existing DDoS tools and their effects. Section VI will cover the DDoSdefense mechanisms at various OSI layers and section VII will show a comparison between the existing defense mechanisms.

II. DDOS: ATTACK VECTOR

In perspective of computer networks, an attack may be defined as an approach to destroy, expose, alter, disable, steal or gain any unauthorized access to an asset. From perspective of DDoS, an attack attempts to misuse the asset.

An attack vector can be defined as a mean by which an attacker can successfully do any of the above attempts by exploiting system vulnerabilities, including human errors.Today there are prevention systems with advanced techniques but one cannot deny the fact that the way DDoS attacks are being performed is evolved with time. This suggests that the attack vector is changing with time. An attack vector will generally fall into one of the categories described below-

A. Volumetric Attacks

In volumetric attack, an attacker attempts to consume the bandwidth within the target network. This assault mostly leads to congestion in the network.

B. TCP State-Exhaustion Attacks

In TCP State-Exhaustion attacks an attacker attempts to consume the connection state tables which are present in many infrastructure components at victim's side.

C. Application Layer Attacks/ Layer 7 Attacks

In Application layer attack, an attacker tries to exploits some of the weaknesses in the application layer protocols such as HTTP, SMTP, DNS, and SIP/VoIP etc. These layer 7 attacks are very dangerous because these attacks are difficult to detect. Simple application layer flood attacks such as HTTP GET flood, HTTP POST flood, etc. have been one of the most common DDoS attacks.

Reference [2] shows that, over the past years the types and sizes of organizations being targeted are broadened substantially. There could be certain reasons for this substantial increase in attacks. Some of the reasons are:

- The awareness, availability and most important, accessibility ofthe tools and techniques that are used to perform DDoS attack.
- Botnets that can be hired on rent basis to perform DDoS attack. There are botnet masters offering a 12k botnet for rent – for the price of $500 per month [9], [10], [11], [12].

III. DDOS: ATTACK STRATEGIES

To conduct the DDoS attack successfully, an attacker needs the following four basic elements [3], [13] :

A. Real attacker

The one who is controlling the entire attack.

B. Master control

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

Master control program works as interface between the real attacker and the Zombies. It also acts as a guard for the zombies that receives the attack command from the real attacker. And it further instructs the zombies to attack on victim.

C. Zombies/slaves/agents

These are compromised systems and these systems are responsible for generating the traffic. These systems have some specific software installed which is being controlled by real attacker via master control.

D. Victim

Targeted host.

With all the above four elements, DDoS attack is carried out in the following four phases [14], [15]:

- *Recruiting/selecting agents:* Agents are nothing but remote machines that are somehow compromised by an attacker, basically to perform actual attack on victim on behalf of attacker. These agents are controlled by exploiting some of the available loop holes or vulnerabilities. Agent machines are chosen in such a way that they should have enough resources to generate powerful attacks. Owner of these machines have no knowledge that their machines have been compromised.
- *Compromising/exploiting:* In this phase, vulnerabilities or security holes of agent machines are exploited by attacker in order to have control over them.
- *Infecting:* In this phase, an attack code is planted in agents machines. In this phase attacker communicate with agents to control the attack.
- *Attack:* In this phase, an attacker commands the start of attack.

IV. DDOS: A CLASSIFICATION

An attacks intend to gain something from a distributed-denial-of-service (DDoS) attack. A DDoS hit is carried out by an attacker with the help of large number interconnected bot computers, known as botnet. Few thousand requests per second are enough to degrade the server's performance. DDoS is relatively easy to generate and is extremely hard to differentiate it from legitimate user traffic. One of the necessary steps towards having an effective DDoSdefense mechanism is to understand the classification of DDoS attack and to develop a defense mechanism accordingly. Various classifications have been proposed over the past decade [5], [15], [16], [17]. Based on the literature survey, DDoS broadly can have six main classifications:

A. Based on Network Protocol Stack

On the basis of protocol DDoS can be further classified as Network/transport level and Application level DDOS attacks as depicted in figure 1. [5].

*1.) Network/transport level DDoSattack :*At this level, mostly TCP, UDP, ICMP, and DNS protocol packets are used to launch the attacks.

*2.) Application level DDoSattack :*These attacks generally consume less bandwidth and are stealthier in nature when compared to volumetric attacks (2.1). However, they can have a similar impact to service as they target specific characteristics of well-known applications such as HTTP, DNS, VoIP or Simple Mail Transfer Protocol (SMTP) [5], [18], [19]. These attacks focus on disrupting legitimate user's services by exhausting the resources [19], [5]. An application-level DDoS attack overloads an application server, such as by making excessive login, database lookup or search requests. Application attacks are harder to detect than other kinds of DDoS attacks.Since the connections are already established and the requests may appear to be from legitimate users. However, once identified, these attacks can be stopped and back-traced to source more easily than any other types of DDoS attacks [19].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

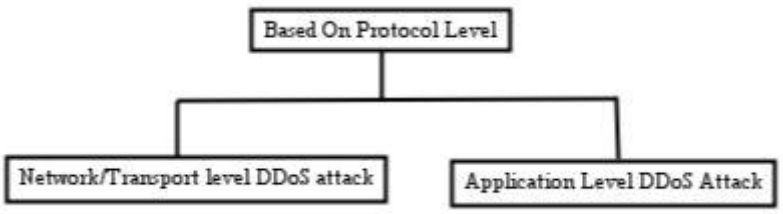

Fig.1DDoS classification based on protocol level

B. DDoS Classification Based on Methodology of Communication

In order to facilitate DDoS attack on computer networks or applications, an attacker mostly uses intermediate agents that are called bots/zombies. These bots are basically compromised computers which are remotely controlled by attacker. The master computer (Attacker's system) communicates with its bots by a command and control channel, which passes the commands from the botmaster to the bots. In response to commands from master computer, bots perform the actual DDOS attack on victim [20]. There can be different ways of communication between botmaster (master computer) and bots (agents/zombies) as depicted in figure 2. On the basis of the methodology of communication, DDoSattacks can be classified asfollow :

1.) Agent-handler based DDoS: The Agent-Handler based DDoS attack consists of clients, handlers, and agents [21]. The attacker basically communicates with client. Then these client systems are used to communicate with agents with the help of some software packages called handlers. Basically agents are also software programs that are installed in compromised systems (bots/zombies) by exploiting the loop holes of the system. These agents will finally carry out the attack, while the real attacker remains at safe side [5], [21], [22].

2.) IRC based DDoS: Internet relay chat (IRC) is a multiuser, online-chatting system that allows users to create two-party or multiparty interconnections and type messages in real time to each other. An IRC based DDoS uses a IRC communication channel to communicate to the agents (bots/zombies) instead of handlers. The agent software will inform the attacker via IRC channel whenever agent (system) become operational.

Benefits of using IRC channels over Agent-handler based channel [21], [23]:

- No need to maintain list of agents because all the available agents can be viewed after entering the IRC server.
- Use of legitimate ports will make traffic legitimate.
- IRC servers have large volume of traffic thereby making it difficult to detect the presence.
- Because this is a centralized approach the major limitation is central point of failure. So if defender captures the IR server, the entire botnet can be shut down [5].

3.) Web based DDoS: Changing the mode of control attackers moved from IRC based communication to websites using HTTP. This shift to a common protocol was a clever move by cyber criminals and malware writers. The exploit kits are developed that can install software on remote machines and then control them from a remote website [24].

Web based control is also a centralized approach but here a number of bots are simply report statics to a website whereas others are intended to be fully configured and controlled through complex PHP scripts and encrypted communications over the 80/443 port and the HTTP/HTTPS protocol. The following are the advantages of Web-based controls over IRC are [21]-

- Ease of set-up and website configuration
- Improved reporting and command functions
- Less bandwidth requirement and the acceptance of large Botnets for the distributed load
- Concealment of traffic and hindrance of filtering through the use of port 80/443
- Resistance to Botnet hijacking via chat-room hijacking, and
- Ease of use and of acquisition

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

4.) P2P based DDoS: More sophisticated communication technique used by attackers is Peer to Peer (P2P) technologies that make use of Peer To Peer protocol, which is an application layer protocol, to carry out DDOS attack. It was in 2007 when first botnet arrived using P2P protocol [24], [25]. In P2P communication botnets are distributed and do not have central point of failure. Comparing to IRC-based botnets, they are more difficult to detect and take down [22].The advantage of a P2P approach is:

- It's distributed which makes it harder to shut down than an IRC-controlled botnet.
- It can provide more stable and robust network.

However, this type is more difficult to maintain and propagate due to its complexity and even Peer-to-peer botnets are hard to develop [24], [26].

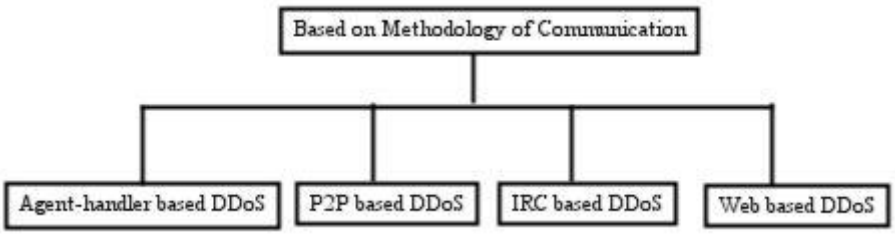

Fig. 2 DDoS classification based on methodology of communication

C. DDoS Classification Based on Exploits

What attacker is going to exploit can be one of the basis of classificationDDoS attacks. On the basis of exploitation of vulnerabilities DDoSattack can be classified as Bandwidth depletion attack and Resource depletion attack [15]:

*1.) A Bandwidth depletion attack :*As the name suggests, it is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the primary victim [17]. This type of attack interrupts the normal working by causing congestion, i.e., exorbitant amount of traffic. Congestion may be due to the total amount of traffic (in bytes), or the total amount of packets (often a lower limit, using short packets) [28]. Here flooding is basically carried out by zombies by sending large amount of traffic to victim's system in order to occupy the entire bandwidth. This can again be categorized as Flood attacks and Amplification attacks as depicted in figure [15], [17], [27].

*2.) A Resource Depletion Attack :*It is basically designed to tie up the resources of a victim system making the victim unable to process legitimate requests for service [17]. An attacker tries to bind the victim's resources by mainly focusing on server or on a particular process. Here attacker can do either of two things:

- Misuse of network protocol communications (protocol exploitation)
- Sending malformed packets

By doing any of the above, attacker can exhaust the available resources [17]. Hence this category can be classified as *Protocol exploitation* and *malformed packet attack*.

3.) A Protocol Exploitation Attack: In protocol exploitation attacks, an attacker uses the existing bugs or some special features of protocols at the victim's system in order to misuse the resources excessively [15], [17], [29].

*4.) Malformed packet attack :*the strategt used in this type of attack is that, an attacker sends defective packets, such as overlapping IP fragments and packets with illegal TCP flags, to a target system, so that the system crashes when it processes such packets [30]. Attacker instructs the agents or zombies or bots to send a large volume of such packets. A malformed packet will cause an application to crash and will also hide subsequent attacker's activities [31], [32]. Malformed attacks are of two types:

- IP address attack

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

- IP packet options attack

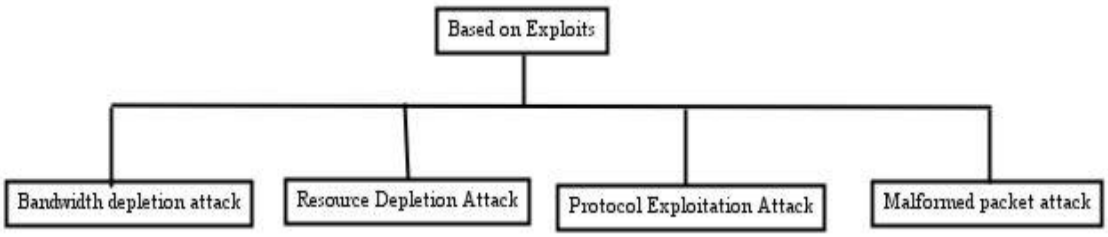

Fig. 3 DDoS classification based on exploits

D. DDoS Classification Based on Attack Methods

One of the basis of classifying DDoS attack can be based on attack methods [15], [16]. There can be two types of attack under this classification –

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

2.) *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], [33].

E. Based on attack rate dynamics

Depending on the attack rate dynamics DDoS attacks can be divided in high rate, low rate, varied rate, continuous rate and variable rate attacks. Low rate DDoS attacks consume lesser resources for long time in contrast to High Rate DDoS attacks which consume more resources for less time [16], [33].

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

2.) *Low Rate attack :*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 A low-rate distributed denial of service (DDoS) attack has significant ability of concealing its traffic because it is very much like normal traffic. It has the capacity to elude the current anomaly-based detection schemes. A low-rate DDoS attack is an intelligent attack as the attacker can send attack packets to the victim at a sufficiently low rate to elude detection [34].

3.) *Varied Rate :*It is a combination of high rate and low rate 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.

4.) *Continuous rate attack:* This consists of attacks that after the onset are executed with full force and without a break or decrement of force. The impact of such an attack is very quick.

5.) *Variable Rate attack*: In variable rate attacks as their name indicates, ''vary the attack rate'' and thus they avoid detection and immediate response. Based on the rate change mechanism one can differentiate between attacks with increasing rate and fluctuating rate. Increasing rate attacks gradually lead to the exhaustion of victim's resources,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

thus delaying detection of the attack. Fluctuating rate attacks have a wavy rate that is defined by the victim's behaviour and response to the attack, at times decreasing the rate in order to avoid detection.

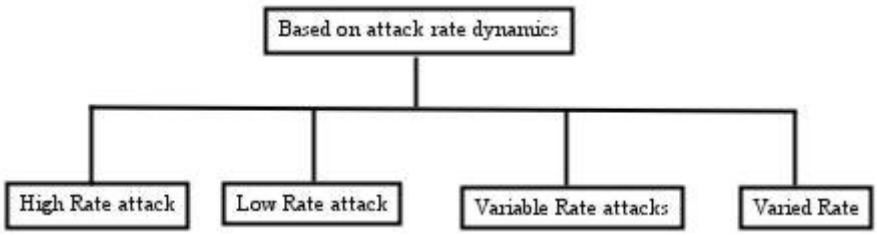

Fig. 4 DDoS classification based on rate of dynamics

F. DDoS Classification Based on degree of automation

Each of the recruit, exploit, infect and attack phases as mentioned in section 3 can be either performed manually or automated. Based on the degree of automation, there can be three types of DDoS attacks:

1.) *Manual*: An attacker manually scans remote machines for vulnerabilities, breaks into them, installs attack code, and then commands the onset of the attack. Only the early DDoS attacks belonged to the manual category. All of the recruitment actions were soon automated.

2.) *Semi-automatic*: In semi-automatic attacks, the DDOS network consists of handler (master) and agent (slave, daemon, zombie, bots) machines. The recruit, exploit and infect phases are automated. In the attack phase, the attacker specifies the attack type, onset, duration and the victim via the handler to agents, who send packets to the victim.

3.) *Automatic DDOS attacks*: Automatic DDOS attacks automate the attack phase in addition to the recruit, exploit and infect phases, and thus avoid the need for any communication between attacker and agent machines. The start time of the attack, attack type, duration and victim are preprogrammed in the attack code. Deployment mechanisms of this attack class offer minimal exposure to the attacker, since he is only involved in issuing a single command at the start of the recruitment process. The hardcoded attack specification suggests a single-purpose use of the DDOS network, or the inflexible nature of the system. However, the propagation mechanisms usually leave a backdoor to the compromised machine open, enabling easy future access and modification of the attack code. Further, if agents communicate through IRC channels, these channels can be used to modify the existing code.

V. EXISTING DDOS ATTACK TOOLS

DDOS attack can be performed by using various available tools. Even one can exploit the systems using their own attacking tool/tools. Easy availability of DDOS tools is one of the reasons for conducting DDoS attack. Some attacking tools are agents based in which agents and handlers know each other's identity while in IRC (Internet relay chat) based attacking tools, communication is done indirectly in which they do not know each other identity.

Using these tools, attackers conceal their identity by the real source of the attackers to stop the attack at the point spoofing the source IP address and launch an attack. The first tools developed to perpetrate the DDoS attack were Trin00 and Tribe Flood Network (TFN) [35], [36]. TFN then bring forth the next generation of tools called Tribe Flood Network 2000 (TFN2K) and Stacheldraht (German for Barb Wire) [38]. These Distributed Denial of Service attack tools are designed to bring one or more sites down by flooding the victim with large amounts of network traffic originating at multiple locations and remotely controlled by a single client . Table I gives a comparison among various popular DDOS tools [39].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

TABLE I
COMPARISON OF DDOS TOOLS

S. No	Tool Name	Reported In Year	Possible Attacks	Packet Format Used To Launch Attacks	Channel Encryption	Model Used
1.	Trinoo [36]	February 2000	Bandwidth Depletion	Udp	Yes	Agent Based
2.	Tfn(Tribe Flood Network) [37]	April 2000	Bandwidth And Resource Depletion	Udp, Tcp-Syn, Icmp Echo Request, Directed Broadcast	No	Agent Based
3.	Tribe Floodnet (Tfn2k) [40]	June 2000	Targa And Mix Attack	Udp, Tcp-Syn, Icmp	Yes	Agent Based
4.	Stacheldraht [38],[41]	June 1999	Bandwidth And Resource Depletion	Udp, Tcp-Syn, Icmp, Directed Broad Cast	Yes	Agent Based
5.	Mstream [42], [43]	April 2000	Bandwidth Depletion	Tcp-Ack, Icmp, Tcp-Rst	No	Agent Based
6.	Shaft [44], [45]	Nivember 1999	Bandwidth And Resource Depletion	Udp, Tcp, Icmp	No	Agent Based
7.	Trinity [46], [47]	August 1999	Bandwidth And Resource Depletion	Udp, Tcp-Syn, Tcp-Ack, Tcp-Rst	No	Irc Based
8.	Knight [48]	July 2001	Bandwidth And Resource Depletion	Syn, Udp	No	Irc Based
9.	Kaiten [48]	August 2001	Bandwidth And Resource Depletion	Udp, Tcp-Syn, Tcp-Push+Ack	No	Irc Based
9.	Owasp Http Post Tool [49]	December 2010	Resource Depletion, Slow Post, Slow Get	Http	No	Agent Based
1o	Davoset [50]	July 2010	Resource Depletion	Xss	No	Agent Based
11	Ufonet [51]	2013	Resource Depletion	Web Abuse	No	Agent Based

VI. DDOSDEFENSE MECHANISMS

The severeness and serious ness of DDoS attack have led to proposal of many defense mechanisms but the complete solution is yet to achieved. This is because, there are certain factors that hinder the advance of DDOS defense research [14]. But usually, the moment DDoS attack is detected, nothing else can be done except for disconnecting the victim from resources. Because any type of reaction will need resources, which are actually already been consumed by DDoS attack, so it is better to drop out the victim from all resources. After the victim is disconnected, the attack source traceback and identification can be carried out. There are number of methods proposed for detecting, trackbacking the DDoS attack attacks [14], [52], [53]. While categorizing DDoS attack defense mechanisms there are several dimensions that are to be kept in mind like location of defense mechanism deployed, protocol level on which defense mechanism works, time when the mechanism is active. These categories can further be classified as depicted in figure:

A. DDoSdefense mechanisms based on deployment

This classification is based on the location of implementation of defense mechanism. This can further be categorize as source based, destination based and network based [14].

1.) *Source based*: Here the mechanisms are deployed near the sources of attack. These mechanisms basically focus on restricting the network customers from generating DDoS attacks. There are various mechanisms that are source based, some major one's are:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

- Ingress/Egress filtering at source's edge router: These techniques are proposed to detect the packets with spoofed IP address at the source's edge router [54].
- D-WARD: D-WARD is a DDoSdefense system deployed at source-end networks that autonomously detects and stops attacks originating from these networks [55].
- MULTOPS: Multi-level tree for online packets statistics as abbreviated MULTOPS is a group of nodes in form of tree structure that contains packet rate statistics. The changes in packet rates are shown by dynamically adapting the shapes [55]. MULTOPS is used by networks at source subnet to detect DDOS flooding attacks.
- MANAnet's reverse firewall: Reverse firewall works in a different way from a traditional firewall. It limits the rate at which it forwards the packets which are not replies [56].

*2.) Destination based :*Under this category, mechanisms are deployed near the victim i.e. either at the edge router or the access router of the destination.

- IP Traceback mechanisms: A technique to identify the origin of the spoofed user is known as the IP Traceback[57],[58],[59],[60],[61].
- Packet marking and filtering mechanisms: In this scheme, legitimate packets are marked so that at the victim's side, a difference can be made between legitimate and attack packets. There are several ways to implement these mechanisms [5],[62],[63],[64],[65],[66],[67],[68]. For example, history based IP filtering [69], Hop-count filtering [70], Path identifier[71], packet dropping based on the level of congestion[72].

*3.) Network based :*These mechanisms are mainly deployed inside networks and on the routers of the autonomous systems [5], [73]. Some of the network based defense mechanisms are route based packet filtering, detecting and filtering malicious routers etc.

B. DDoSdefense mechanisms based on protocol

Under this category the defense mechanisms can be classified as the mechanisms to defend against the TCP/NETWORK level DDOS attacks and mechanisms to defend against APPLICATION level DDOS attacks.

1.) TCP: These types of mechanisms are basically deployed to defend against DDoS attacks where TCP protocol is exploited. Some of the common defenses are[74]:

- Filtering: The filtering techniques represent the best current practices for packet filtering based on IP addresses
- Increasing Backlog: This technique focuses on use of large backlogs so that in case TCB buffers are exhausted, backlogs can be used.
- Reducing SYN-RECEIVED Timer: Another quickly implementable defense is shortening the timeout period between receiving a SYN and reaping the created TCB for lack of progress. A shorter timer will keep bogus connection attempts from persisting for as long in the backlog and thus free up space for legitimate connections sooner.
- Recycling the Oldest Half-Open TCB: Once the entire backlog is exhausted, some implementations allow incoming SYNs to overwrite the oldest half-open TCB entry. This works under the assumption that legitimate connections can be fully established in less time than the backlog can be filled by incoming attack SYNs.
- SYN Cache: Here the server node has a global hash table to keep half-open states of all applications, while in the original TCP these are stored in the backlog queue provided for each application. As a result, the node can have a larger number of half-open states and the impact of a SYN flood attack can be reduced.
- SYN Cookies: SYN cookies modify the TCP protocol handling of the server by delaying allocation of resources until the client address has been verified. This technique used to guard against SYN flood attacks. The use of SYN Cookies allows a server to avoid dropping connections when the SYN queue fills up. Instead, the server behaves as if the SYN queue had been enlarged. The server sends back the appropriate SYN+ACK

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

response to the client but discards the SYN queue entry. If the server then receives a subsequent ACK response from the client, the server is able to reconstruct the SYN queue entry using information encoded in the TCP sequence number.

- Hybrid Approaches: The SYN cache and SYN cookie techniques can be combined. For example, in the event that the cache becomes full, then SYN cookies can be sent instead of purging cache entries upon the arrival of new SYNs. Such hybrid approaches may provide a strong combination of the positive aspects of each approach.
- Firewalls and Proxies: Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses. Some DDoS attacks are too complex for today's firewalls, e.g. if there is an attack on port 80 (web service), firewalls cannot prevent that attack because they cannot distinguish good traffic from DDoS attack traffic. Additionally, firewalls are too deep in the network hierarchy. The router may be affected even before the firewall gets the traffic. Nonetheless, firewalls can effectivel prevent users from launching simple flooding type attacks from machines behind the firewall.

2.) *IP level defense mechanism:* These defense mechanisms are used as countermeasure to IP-Level DDoS attacks.

Following are some defense mechanisms.

- SIP defender: VoIP Defender, an open security architecture that is designed to monitor the traffic flow between SIP servers and external users and proxies. The goal is to detect attacks directed at the protected SIP server and provide a framework for attack prevention / mitigation [75], [76].
- Push back: Pushback is a mechanism for defending against distributed denial-of-service (DDoS) attacks at IP level. It is a mechanism that allows a router to request adjacent upstream routers to limit the rate of traffic [77], [78].
- Puzzle based approaches: In this defense mechanism cryptographic puzzles are used as a countermeasure to low level denial of service attack such as IP-Layer flooding [79].

3.) *Application level defense mechanisms:* These defense mechanisms are implemented to defend against application level attack. Because http level attack is more difficult to trace due to its legitimate behavior. Amount of traffic used to successfully carry out application level DDoS is much less than to carry out a TCP or IP level DDoS attack. That is why the techniques used to detect TCP or IP level DDoS attacks are incapable to detect application level DDOS attacks. Application level defense mechanisms can be:

- Mitigation on the page access behavior: On the basis of page access behavior, HTTP-flooding can be defended [20].
- DDOS shield: Here statistical methods are used to detect HTTP level DDOS attacks [19].
- Defense against tilt DDOS attacks: This monitors a user's features (e.g. request volume, instant and long-term behavior) throughout a connection session to determine whether he is malicious user or not [80].

C. DDOS defense mechanisms based on time of action

Based on the time of action, defense mechanisms can be of following types:

1.) *Before the attack:* These attack mechanisms are basically deployed to prevent the attack from happening. Most of these mechanisms are focused on fixing the bugs such as protocol exploits system vulnerabilities etc. There are many mechanisms mentioned in [5].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

2.) *During the attack:* After the prevention of attack, now its turn to detect the attack. Mechanisms in this category are deployed to detect the attack when it happens. There are various methods to detect the attack. IDPS systems or firewalls can be used under this category.

3.) *After the attack:* These mechanisms are deployed to act once the DDOS is detected and to trace back the source of attack.

VII. COMPARISION OF DDOSDEFENSE MECHANISMS

Defense mechanisms discussed in section 6 have both advantages and some shortcomings. There also exists significant difference between these mechanisms either due to the layer of applicability or due to their way or defending. Table II gives the advantages and shortcomings of some of the defense mechanisms.

TABLE II
COMPARISION OF DDOS DEFENSE MECHANISMS

S.No	Defense Mechanisms	Advantages	Shortcomings
1	Ingress/Egress filtering at source's edge router	Detect and filter packets with spoofed IPaddresses at the source's edge routers based on the valid IPaddress range internal to the network	Spoofedpackets will not be detected if their addresses are still in the Valid internal IP address range
2	D-WARD	Stop attack traffic originating From a network at the border of the source network	It consumes more memory space and CPUcycles than some of the network-based defense mechanisms
3	MULTOPS	Detects and filtersddosflooding attacks based on significant difference between therates of traffic going to and coming from a host or subnet	It uses a dynamic tree structurefor monitoring packet rates for each IP address which makesit a vulnerable target of a memory exhaustion attack
4	MANAnet's reverse firewall	Limits the rate at which it forwards packets thatare not replies to other packets that recently were forwardedin the other direction	It is manual and requires the administrators'involvement
5	IP Traceback mechanisms	Traces back the forged IP packets to their true sources ratherthan the spoofed IP addresses	Serious deploymentand operational challenges, most of thetrace back mechanisms have heavy computational, network ormanagement overheads
6	Packet marking and filtering mechanisms	Mark legitimate packetsat each router along their path to the destination so thatvictims' edge routers can filter the attack traffic	Dependent in part on the strength of the attackers, andwhen it increases, filters become ineffective and they cannotproperly be installed
7	Increasing Backlog	Helps in defending against overflowing a host's backlog of connecting sockets	Solution is known to be a poor one because of the use of linear list traversal in the functions that attempt to free state associated with stale connection attempts

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

8	Reducing SYN-RECEIVED Timer	Put a tighter limit on the amount of time between when a TCB enters the SYN-RECEIVED state and when it may be reaped for not advancing	In cases of aggressive attacks that impose some amount of congestion loss in either the SYN-ACK or handshake-completing ACK packets, legitimate connection tcbsmay be reaped as hosts are in the process of retransmitting these segments
9	Recycling the Oldest Half-Open TCB	Allow incoming synsto overwrite the oldest half-open TCB entry once entire backlog is exhausted	Fail when the attacking packet rate is high and/or the backlog size is small, and is not a robust defense.
10	SYN Cache	Effective because the secret bits preventan attacker from being able to target specific hash values,	Complex in nature
11	SYN Cookies	Causes absolutely zero state to be generated by a received SYN	Not all TCB data can fit into the 32-bit Sequence Number field, so some TCP options required for high performance might be disabled SYN-acksare not retransmitted because retransmission would require state
12	Firewalls and Proxies	Defend against SYN flooding attacks	Can be easily bypassed using advance mechanisms
13	IP level defense mechanism	Dedicated to protect SIP servers	Complex to implementWorks only at ip level
14	Mitigation on the page access behavior	Prevent HTTP-GET flooding attacks	Large False positives

VIII. CONCLUSION

To the best of our knowledge, our survey study is the first of its kind to study and compare DDoS tools and defense mechanisms evolved over the period of time. With the evolution of attacks, it is observed that various counter-measures are proposed and are implemented. Survey study will help security professionals to analyse the attack strategies and to come up with robust security solutions.

REFERENCES

1. http://en.wikipedia.org/wiki/Cyberspace
2. http://www.arbornetworks.com/attack-DDoS
3. Anupama Mishra, B.B.Gupta and R.C.Joshi, "A Comparative study of Distributed Denial of Service Attacks, Intrusion Tolerance and mitigation Techniques", 2011 European Intelligence and Security Informatics Conference
4. L. Garber, "Denial-of-service attacks rip the Internet," IEEEComputer, Volume 33, Issue 4, pp. 12–17, Apr. 2000.
5. SamanTaghaviZargar, James Joshi and David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION
6. http://www.bankinfosecurity.in/DDoS-hacktivists-no-us-bank-safe-a-5401/op-1
7. Prolexic Quarterly Global DDOS attack report Q1 2013
8. http://www.securelist.com/en/blog/208194203/The_Biggest_DDoS_Ever_that_Almost_Broke_the_Internet
9. https://blog.damballa.com/archives/330
10. http://blog.webroot.com/2012/06/06/DDoS-for-hire-services-offering-to-take-down-your-competitors-web-sites-going-mainstream/
11. http://blog.executivebiz.com/2010/09/chinese-botnet-herders-offer-commercial-DDoS-services/
12. http://www.incapsula.com/DDoS/DDoS-attacks/botnet-DDoS

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

13. Aarti Singh, Dimple Juneja, "Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks", International Journal of Engineering Science and Technology Vol. 2(8), 2010, 3405-3411
14. JelenaMirkovic, Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms"
15. Christos Douligeris, AikateriniMitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art", Department of Informatics, University of Piraeus, 80 Karaoli and DimitriouStr, Piraeus 18534, Greece Received 9 October 2003; accepted 13 October 2003 Responsible Editor: I.F. Akyildiz
16. ShuchiJuyal, RadhikaPrabhakar, "A COMPREHENSIVE STUDY OF DDOS ATTACKS AND DEFENSE MECHANISMS", Journal of Information and Operations Management.
17. Stephen M. Specht, Ruby B. Lee, "Distributed Denial of Service:Taxonomies of Attacks, Tools and Countermeasures",
18. Arbor Application Brief, The Growing Threat of Application-Layer DDoS Attacks",
19. SupranamayaRanjan, Ram Swaminathan, Mustafa Uysal, Edward Knightly, "DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection"
20. Lei Zhang, Shui Yu, Di Wu, Paul Watters, "A Survey on Latest Botnet Attack and Defense", 2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11
21. EsraaAlomari, SelvakumarManickam, ,B. B. Gupta, Shankar Karuppayah, RafeefAlfaris, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art", International Journal of Computer Applications (0975 – 8887) Volume 49– No.7, July 2012
22. Jing Liu, Yang Xiao, KavehGhaboosi, Julia Deng, Jingyuan Zhang, "Botnet: Classification, Attacks, Detection,Tracing, and Preventive Measures", Submitted to EURASIP Journal on Wireless Communications and Networking, (under revision)
23. K. J. Houle, "Trends in Denial of Service Attack Technology," CERT Coordination Center, Carnegie Mellon Software Engineering Institute, oct 2001.
24. Zheng Bu, Pedro Bueno, Rahul Kashyap, and Adam Wosotowsky, "The New Era of Botnets", McAfee Labs
25. David Dittrich, Sven Dietrich, "P2P as botnet command and control: a deeper insight"
26. http://security.stackexchange.com/questions/2440/why-do-botnets-use-irc-but-not-a-web-service-for-communication
27. http://www.nexusguard.com/resourcesDDoS.htm
28. MotiGeva, Amir Herzberg, YehoshuaGev, "Bandwidth Distributed Denial of Service: Attacks and Defenses",
29. NirbhayAhlawat, Chetan Sharma, "Classification and Prevention of Distributed Denial of Service Attacks", INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES Vol No. 3, Issue No. 1, 052 – 060
30. http://www.h3c.com/portal/Products___Solutions/Technology/Security_and_VPN/Technology_White_Paper/200804/604013_57_0.htm
31. http://en.wikipedia.org/wiki/IP_fragmentation_attacks
32. http://www.isi.edu/~mirkovic/bench/attacks.html
33. NehaTewari ,AkashBhardwaj, "Flow Statistics Based Detection of Low Rate and High Rate DDoS Attacks", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 348 ISSN 2229-5518
34. Yang Xiang, Member, Ke Li, and Wanlei Zhou, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics"
35. P.J. Criscuolo, Distributed Denial of Service Tools Trinoo, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht
36. http://staff.washington.edu/dittrich/misc/trinoo.analysis
37. http://staff.washington.edu/dittrich/misc/tfn.analysis
38. http://staff.washington.edu/dittrich/misc/stacheldraht.analysis
39. Arun Raj Kumar, P. , S. Selvakumar, "Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment A Survey on DDoS Attack Tools and TracebackMechanisms",IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009
40. http://www.cert.org/incident_notes/IN-99-07.html#tfn
41. http://www.iss.net/threats/advise43.html
42. http://www.cert.org/incident_notes/IN-2000-05.html
43. http://www.iss.net/security_center/reference/vuln/DDoS-mstream-zombie.htm
44. https://www.usenix.org/legacy/events/lisa00/full_papers/dietrich/dietrich_html/
45. http://www.pestpatrol.com/zks/pestinfo/a/analysis_of_the_shaft_DDoS_tool.asp
46. http://www.iss.net/security_center/reference/vuln/IRC_Trinity.htm
47. Michael Marchesseau, "Trinity" - distributed denial-of-service attack tool, Global Information Assurance Certification Paper
48. http://www.scribd.com/doc/43533237/57/DDoS-Tool-Knight-and-Kaiten
49. https://www.owasp.org/index.php/OWASP_HTTP_Post_Tool
50. http://websecurity.com.ua/davoset/
51. http://ufonet.sourceforge.net/
52. L. C. Chen, T. A. Longstaff, K. M. Carley, "Characterization of defense mechanisms against distributed denial of service attacks", Computers & Security, vol. 23, no. 8, pp. 665-678, December 2004.
53. T. Peng, C. Leckie, and K. Ramamohanarao," Survey of network-based defense mechanisms countering the DoS and DDoS problems", ACM Comput. Surv. 39, 1, Article 3, April 2007.y
54. P. Ferguson, P. Ferguson, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing"
55. JelenaMirkovi´c Gregory Prier Peter Reiher, "Attacking DDoS at the Source"
56. www.cs3-inc.com/pubs/ps_MANAnet-Reverse-Firewall.pdf
57. ZeeshanShafi Khan, Nabila Akram, KhaledAlghathbarl, Muhammad She, RashiMehmood, "Secure Single Packet IP Traceback Mechanism to Identify the Source"

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

58. N.Srilakshmi1, K.Rani, "AN IMPROVED IP TRACEBACK MECHANISM FOR NETWORY SECURITY"
59. Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, "Practical Network Support for IP Traceback"
60. Lakshmi Santhanam, Anup Kumar and Dharma P. Agrawal, "Taxonomy of IP Traceback"
61. RIM: Router Interface Marking for IP TracebackRuiliang Chen, Jung-Min Park, and Randolph Marchany
62. Chao Gong, KamilSarac, "IP Traceback based on Packet Marking and Logging"
63. Zhao Deshan, Cao Bin," Research on the Algorithm of Data Packet Marking for DDoS Attack"
64. Lin Chen, Ming He, Zhihong Liu, Guilin Cai, "A New Active Path Identification and Filtering Method", 2013 27th International Conference on Advanced Information Networking and Applications Works.
65. SamantSaurabh, Ashok Singh Sairam, " Linear and Remainder Packet Marking for Fast IP TraceBack"
66. Wei Yen, Cyclical Deterministic Packet Marking, 1-4244-0991-8/07/$25.00/©2007 IEEE
67. Basheer Al-Duwairi, ManimaranGovindarasu , "Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 17, NO. 5, MAY 2006
68. SamantSaurabh, Ashok Singh Sairam , "A More Accurate Completion Condition for Attack-Graph Reconstruction in Probabilistic Packet Marking Algorithm", 978-1-4673-5952-8/13/$31.00 c 2013 IEEE
69. Tao Peng, Christopher Leckie, KotagiriRamamohanarao, "Protection from Distributed Denial of Service Attack Using History-based IP Filtering", story-based IP filtering, ICC '03.May , Vol.1, pp: 482- 486, 2003
70. Haining Wang, Cheng Jin, Kang G. Shin, " Defense Against Spoofed IP Traffic Using Hop-Count Filtering",
71. A. Yaar, A. Perrig, and D. Song, Pi: A Path Identification Mechanism to Defend against DDoS Attacks, in IEEE Symposium on Security and Privacy, pp. 93, 2003
72. Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao, PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks, IEEE Trans. Dependable Secure Computing, vol. 3, no. 2, pp. 141-155, 2006
73. E. Y. K. Chan et al., Intrusion Detection Routers: Design, Implementation and Evaluation Using an Experimental Testbed, IEEE J. Sel. Areas Commun., vol. 24, no. 10, pp. 1889 - 1900, 2006.
74. http://tools.ietf.org/html/rfc4987
75. Jens Fiedler, Tomas Kupka, Sven Ehlert, Prof. Dr. Thomas, Dr. DorghamSisalem, "VoIP Defender: Highly Scalable SIP-based Security Architecture"
76. Felipe Huici, SaverioNiccolini, Nicod'Heureuse, "Protecting SIP against Very Large Flooding DoS Attacks", NEC Europe Ltd.
77. John Ioannidis, Steven M. Bellovin, "Implementing Pushback: Router-Based Defense AgainstDDoS Attacks"
78. Tao Peng, Christopher Leckie, KotagiriRamamohanarao, "Defending Against Distributed Denial of Service Attacks Using Selective Puchback"
79. Brent R. Waters, Ari Juels, chrissTunnell, Edward W. Felten, "Puzzle Outsourcing for IP-Level DoS Resistance"
80. Huey-Ing Liu, Kuo-Chao Chang, "Defending Systems Against Tilt DDoS Attacks", The 6th International Conference on Telecommunication Systems, Services, and Applications 2011