Research Journal of Applied Sciences, Engineering and Technology 8(8): 995-1001, 2014
DOI:10.19026/rjaset.8.1061
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: April 26, 2014 Accepted: June 08, 2014 Published: August 25, 2014

Research Article

A Survey of DDOS Attacks in TCP/IP Stack

[1]P.C. Senthil Mahesh and [2]Paul Rodrigues
[1]Department of CSE, Dhaanish Ahmed College of Engineering, Anna University, Chennai,
[2]DMI College of Engineering, Chennai, Tamilnadu, India

Abstract: The aim of study is to discuss DDOS attack in TCP/IP layer. A Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attack is an attempt to make a device or network source not available to its designed customers. The purposes and objectives of a DoS attack may differ, it usually includes initiatives to momentarily or consistently disrupt or hold solutions of a variety linked with the Online. As explanation, DDoS (Distributed Denial of Service) attack are sent by two or more individuals, or bots. DoS (Denial of Service) attack are sent by one person or system. DoS attack typically focus on sites or solutions organized on high-profile web or web servers such as financial institutions, bank card payment gateways and even main name servers. This technique has now seen comprehensive use in certain activities, used by server owners, or dissatisfied opponents on activities. Progressively, DoS attack have also been used as a way of level of resistance.

Keywords: DDOS, network attacks, TCP/IP

INTRODUCTION

In computer and computer networks an attack is attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or makes unauthorized use of an asset (Palmieri *et al*., 2011).

The goal of a denial of service attack is to deny legitimate users access to a particular resource. An incident is considered an attack if a malicious user intentionally disrupts service to a computer or network resource. Resource exhaustion (consume all bandwidth, disk space).

Distributed Denial-of-Service attack (DDoS attack) is a try to make a machine or network resource inaccessible to its deliberate users (Ricciardi *et al*., 2011). It causes to the Internet temporarily or frequently disturb or interrupt services by sending the continues request. Denial-of-service attacks are deliberated breaches the architecture of internet and it also violate the acceptable use policies Internet service providers.

DDoS attacks can seriously damage the Internet service. In late June and early July of 1999 the first DDoS attack was observed. In August 1999 the first well-documented DDoS attack occurred, when a DDoS tool called Trinoo was organized in at least 227 systems, of which at least 114 were on Internet 2, to flood a single University of Minnesota computer; this system was cracked off the air for more than 2 days (Stephen and Ruby, 2003). In February 2000 the first well-DDoS attack was publicized in the public press. On February 7, Yahoo! Internet portal was unreachable for 3 h because of DDoS. During this attack Yahoo was down, it suffered a loss of e-commerce and marketing revenue that amounted to about $50,000. (Carl *et al*., 2006) During the DDoS attacks, Buy.com went down from 100% availability to 9.4% and also CNN.com's client went down to below 10% of normal value. The downtime loss was huge (Bellovin *et al*., 2001).

The websites of Google, Yahoo and Microsoft was affected by DDoS attack on June 2004, vanished for hours when their servers were saturated with thousands of simultaneous webpage requests that they could not handle request (Malan *et al*., 2000). These webpage requests are from botnet which consists of thousands of infected machines. Before the attack, the attacker tried to scan the Internet to find out the vulnerable machines and fix the bot on those machines. Internet relay chat rooms are used for communication between the attacker and those zombie machines. After the attacker issued the attack command in an Internet relay chat room, the botnet start to generate a large number of web requests which bring down the victim websites. These kinds of botnets are increasing a crime wave against e-commerce.

The attacks weren't coming from selected "bot" computers, as is common. Instead, its machines were under attack by DNS (Domain Name System) servers. The new kind of attack is, an attacker will use a botnet to send a more number of request to open DNS servers. These queries will be "spoofed" to look like they come

Corresponding Author: P.C. Senthil Mahesh, Department of CSE, Dhaanish Ahmed College of Engineering, Anna University, Chennai, Tamilnadu, India

Table 1: Different types of attacks in TCP/IP layers

Two categories of attack based on protocol	Different types of attack
Transport level-DDoS flooding Attacks	• Flooding attacks • Protocol exploitation flooding attacks • Reflection-based flooding attacks • Amplification-based flooding attacks
Application level-DDoS flooding attacks	• Reflection/amplification based flooding attacks • HTTP flooding attacks o Session flooding attacks o Request flooding attacks o Asymmetric attacks o Multiple HTTP get/post flood o Faulty application • Slow request/response attacks o Slowloris attack o HTTP fragmentation attack o Slowpost attack o Slowreading attack
Nerwork level DDos flooding attacks	• Black hole attack • Gray hole attack • Byzantine attack • Warm hole attack • Information is closure • Message tampering • Routing attack
Physical level DDos flooding attacks	• Direct attack • Indirect attack • Psudeo attack
Botnet-based DDOS attacks	• IRC-based • Web-based • P2P-based
The defense mechanisms against network/transport-level DDoS flooding attacks	• Source-based o Ingress/egress filtering at the sources' edge routers o D-WARD o Multi-Level Tree for Online Packet Statistics (MULTOPS) and Tabulated Online Packet Statistics (TOPS) o MANAnet's reverse firewall • Destination-based o IP traceback mechanisms o Management information base o Packet marking and filtering mechanisms o History-based IP filtering o Hop-count filtering o Path identifier o Packet dropping based on the level of congestion • Network-based o Route-based packet filtering o Detecting and filtering malicious routers • Hybrid o Hybrid packet marking and throttling/filtering mechanisms o Aggregate-based Congestion Control (ACC) and pushback o Attack Diagnosis (AD) and parallel-AD o TRACK o Defensive Cooperative Overlay Mesh (DEFCOM) o Cossack o Capability-based mechanisms o Active Internet Traffic Filtering (AITF) as a filter-based (datagram) mechanism o StopIt
The defense mechanisms against application-level DDoS flooding attacks	• Destination-based o Defense against reflection/amplification attacks o DDoS-shield o Anomaly detector based on hidden semi-Markov model o DAT (Defense Against Tilt DDoS attacks) • Hybrid o Speak-up o DOW (Defense and Offense Wall) o Differentiate DDoS flooding bots from human o Admission control and congestion control o TMH (Trust Management Helmet) o Hybrid detection based on trust and information theory based metrics

Table 1: Continue

Two categories of attack based on protocol	Different types of attack
Response criterion of defense mechanisms against flooding attack.	● Before the attack (attack prevention) ○ System and protocol security mechanisms to increase the overall security of the systems ○ Fail-safe protection ○ Resource allocation and accounting ○ Reconfiguration mechanisms ○ Installing firewalls and improved Intrusion Detection & Prevention Systems (IDPSs) ○ Employing local filters ○ Load balancing and flow control ○ Server-side specific security considerations ● During the attack (attack detection) ● After the attack (attack source identification and response) ○ Attack source identification ○ Initiating a proper response

from the target address and the DNS server will reply to that network address. Using DNS servers to do their illegitimate work offers key helps to attackers. It hides their original systems address, making it difficult for the victim to find the original source of the attack. But more important, reflecting an attack through a DNS server also allows the assault to be improved, providing a larger amount of malicious traffic to the target. A single DNS query could initiate a reply that is as much as larger than the request. To protect the DNS servers it should be configured to only provide DNS services to machines within a trusted domain and it reduce the abuse and prevent this kind of attack. DNS servers restricting recursion and restricting the ability to send additional delegation information can to prevent DNS-based DDoS attacks (Abadi *et al*., 2003; Abdelsayed *et al*., 2003) (Table 1).

The number of DDoS (Distributed Denial-of-Service) attacks mark the inadequate sites in Web applications and network services. Attackers are using complicated methods to avoid defenses according to DDoS modification experts. To classify defense mechanism against network and application level DDoS flooding attack based on the location where prevention detection and response to DDoS flooding attack occurred.

TRANSPORT LEVEL-DDOS FLOODING ATTACKS

These type of attack occurred by TCP, UDP, ICMP and DNS protocol packets.

Flooding attack: Attacker sends requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

Protocol exploitation flooding attacks: Attacker creates some special features and bugs in the victim protocol. So it will destroy the victim resources.

Reflection-based flooding attacks: Attackers send the forged request to the different service provider with the target IP address, requested service provider will send the replay to the target. So the target resource will be exhausted.

Amplification-based flooding attacks: Attacker sends the large number of message to a victim's. It will create a flood of traffic on a victim.

Application level-DDOS flooding attacks: This Type of attack focus on disturbing right user's services by killing the server resources.

Reflection/amplification based flooding attacks: These attacks are same as Network level attack. But here instead of network level to use application level request to the zombies. The attacker sends the DNS query to the forged IP address. So it will send the DNS response. DNS query message is larger than DNS response message.

HTTP flooding attacks: Attacker sends the Http request to a victim web server.

Session flooding attacks: Attacker sends the large number request to the service provider. The number request came from attacker is larger compared to right user.

Request flooding attacks: This type of attack attacker sends a single session that contains more number of requests. This attack is varied from HTTP get/post attack because it will support HTTP 1.1.

Asymmetric attacks: Attacker sends the session it contain large number of message.

Multiple HTTP get/post flood: Attacker sends multiple requests with in single session to the victim. The message has to be send one after another.

Faulty application: Attacker generates the SQL. Injection query it will lockup the database queries. These attacks occurred at poor web design and improper integration of database.

Slow request/response attacks: Attacker can generate high workload request with in single session.

Slowloris attack: Slowloris attack is defined as the attacker use limited number of machine or a single machine for web server. The attacker sends only partial request.

HTTP fragmentation attack: The attacker brings down the web server by connecting the HTTP request for a long period of time without any alert information.

The HTTP request is fragment into small instance and sends it to victim as the valid HTTP request.

Slow post attack: The HTTP post command brings down the web server. The attackers send the complete HTTP request it contain content length. The server waits for each message so it will slow down the process.

Slow reading attack: This type of attack work as slowly reading the response message.

Network level DDOS flooding attacks: To create a Network layer DoS attack, most attackers pound a target network with more data than it can handle. Falling behind, the target network begins to slow and drop packets, which may or may not cause a flood of retransmission requests. Bandwidth is soaked up and the network becomes unusable for all users.

Black hole attack: A packet drop attack or blackhole attack is a type of denial-of-service attack in which a router that is expected to pass on packages instead discards them. This usually happens from a wireless router becoming affected from a variety of different causes.

Gray hole attack: Gray hole attack is either to drop the packet selectively or drop the packet randomly.

Byzantine attack: A affected advanced node performs alone, or a set of affected advanced nodes performs in collusion and carry out attacks such as developing redirecting loops, sending packages through non-optimal routes, or precisely losing packages, which results in interruption or deterioration of the redirecting services.

Warm hole attack: Colluding attackers uses “tunnels” between them to forward packets. Place the attacker in a very powerful position. The attackers take control of the route by claiming a shorter path.

Information closure: The infected nodes are gaining the confidential information and pass it into unauthorized users.

Message tampering: Attacks describe attacks where an attacker alters the data sent between a web service client and web service receiver. The attacker changes the SOAP message in transit and therefore violates the security objective of "Integrity".

Routing attack: Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols.

Physical level DDOS flooding attacks: Physical security ensures that the data have a minimum privacy and Quality of Service (QoS) and that the users are informed when such conditions are violated.

Direct attack: Characteristics of certain physical link elements are more likely to be intruded and exploited as direct attack ports.

Indirect attack: Certain network elements are more likely to be attacked indirectly, because it is too complicated to attack them directly, or they are not easily accessible. This type of attacks include:

- Indirect crosstalk
- Unauthorized access through add/drop ports
- Intentional crosstalk propagation from preceding blocks

Pseudo-attacks: Anomalies which are not intrusions, but may be interpreted as such, due to significant changes in the signal quality depending on the physical network design.

Botnet-based DDOS attacks: Botnet is defined as it is the group of zombies controlled by an attacker. Attacker can be installed the program into the infected system and the attacker communicate with to sending the command.

IRC-based: IRC is a text based online message. It has client and server architecture. It handles hundreds of client through multiple servers. Server contains the list of client details. The attacker installs the botnet in the server and sends the message by using Command and Control (C and C) fashion. Trinity and Kaiten are the some of the botnet tool.

Web-based: Web based botnets are communicate by HTTP request. Web bots are periodically downloading the file. So it will make them traffic.

DEFENSE MECHANISMS AGAINST NETWORK/TRANSPORT-LEVEL DDOS FLOODING ATTACKS

Some techniques are used to prevent the DDOS flooding attack.

Source-based mechanisms: This technique is performed at the source side. These mechanisms take place at routers of the source's local network or at the access routers of an Autonomous System (AS).

Ingress/egress filtering at the sources' edge routers: This filtering method performed at the source side. It will filter the spoofed IP address within the network. It will allow only the valid IP address.

D-WARD: It is used to detect the DDOS flooding attack. It will monitor the bound and inbound traffic. The network contain predefined normal flow model. If the infection is found out then it will compared with normal flow.

Multi-Level Tree for Online Packet Statistics (MULTOPS) and Tabulated Online Packet Statistics (TOPS): MULTOPS and Tops are designed in the basis of incoming and outgoing packets rate are proportional. MULTOPS are heuristic and data structure. Tops are design in the form of heap structure.

MANAnet's reverse firewall: Traditional firewall, which protects a network from incoming packets. The reverse firewall protects the outside from packet flooding attacks that originate from within a network. A reverse firewall limits the rate at which it forwards packets that are not replies to other packets that recently were forwarded in the other direction.

Destination-based mechanisms: This mechanism allow at the destination side. The edge routers are installed at the destination.

IP traceback mechanisms: The IP Traceback technique is defined as trace back the original IP address from the spoofed IP address.

Management information base: MIB contain the parameter which includes various packet format and specified path.

Packet marking and filtering mechanisms: This mechanism allow the user can mark the correct packet with the particular specified route. So it will reduce the traffic.

History-based IP filtering: The destination host contains the list of frequently used IP address list. If new request will come from source then it will compare to the list and block the new IP address.

Hop-count filtering: In this type of filtering, the source IP address and the number of hop from source to destination is stored into destination side. It will used for comparing at the time of attack.

Path identifier: To mark the different path for each and every packet.

Packet dropping based on the level of congestion: If any congestion will occur then the host will leave the particular packet.

Network-based: This mechanism mainly focuses on within the network. The detection technique performed at the intermediate node of network.

Route-based packet filtering: Suddenly a new source address appears in an IP packet on a link, then it is assumed that the source address has been spoofed and hence the packet can be filtered.

Detecting and filtering malicious routers: Watchers are a new algorithm used to detect malicious packet at the time of communication.

Hybrid: This mechanism allow both client and server side. Detection can be performed at the server side and distribute to the client for proper response. It is called centralized mechanism.

Hybrid packet marking and throttling/filtering mechanisms: This type of attack both client and server are used. The detection technique will be placed in the target and filtering mechanism will be used at source.

Aggregate-based Congestion Control (ACC) and pushback: ACC rate limits the combination IP sources. Aggregates are subsets of traffic defined as some characteristics such as specific destination port or source IP address. In ACC, routers detect aggregates that are crushing them by using samples of packet drops in their queues. Then they send a pushback message to the upstream routers along with the information about the aggregates to request a rate limit by presenting a rate limit value.

Attack Diagnosis (AD) and parallel-AD: AD is the combination of pushback and packet marking concept. The target host activates the AD after detecting the attack. It will send the command by an upstream link. After receiving the command it will mark the packet and record the information.

Track: This mechanism allow combination IP traceback, packet marking and packet filtering. TRACK is the combination of two components: router port marking module and packet filtering module. The router port marking module marks packets by locally unique 6-digit identifier, to the packets it transmits. If the path is attacked, after receiving the packets marked by each router, a victim machine can then use the information contained in those packets to trace the attack back to its source. Then, the packet filtering component employs the information contained in the same packets to filter the malicious packets at the upstream routers, thus effectively mitigating attacks.

Defensive Cooperative Overlay Mesh (DEFCOM): It will distribute all the information and service exchange to the defense node.

Cossack:
Capability-based mechanisms: This mechanism allows how to handle the large number traffic at a destination. It will discard the unsecure data. The memory cost and performance are high.

Active Internet Traffic Filtering (AITF) as a filter-based (datagram) mechanism: Capability-based mechanisms allow a receiver to reject by default all the traffic and explicitly accept only the traffic that belongs to recognized network-layer connections. The alternative approach is datagram mechanism in which a receiver accepts by default all the traffic and explicitly rejects the traffic that has been identified as unwanted.

StopIt: It is a hybrid filter-based DDoS defense mechanism that allows each receiver to install a network filter that blocks the unwanted traffic it receives. StopIt uses Passport as its secure source authentication system to prevent source address spoofing.

The defense mechanism against application-level DDoS flooding attacks:
Destination-based: A server is a process that implements a specific service. A client is a process that requests a service from a server.

Defense against reflection/amplification attacks: Defense against Reflection/Amplification attacks are same as Network Level reflection mechanism. But here DNS queues are make heavy traffic in the network link.

DDoS-shield: This mechanism focus on statistical methods to detect the HTTP sessions and services rate-limiting as the primary defense mechanism. DDoS-Shield consists of a several assignment mechanism and a DDoS-resilient scheduler. The suspicion assignment mechanism assigns a continuous value as opposed to a binary measure.

Anomaly detector based on hidden semi-markov model: By using anomaly detector to find out the attack with the help of dynamically changing of matrix. The main disadvantage of this mechanism is complexity of algorithm.

DAT (Defense Against Tilt DDoS attacks): It will monitor the HTTP connection throughout the communication and it will determine whether the new user is attacker or not.

Hybrid: This mechanism allow both client and server side. Detection can be performed at the server side and distribute to the client for proper response.

Speak-up: This mechanism tries to reduce the number of malicious request.

DOW (Defense and Offense Wall): This mechanism allows K-means clustering techniques. It will analyze and detect the attack based on anomaly detection.

Differentiate DDOS flooding bots from human: This technique differentiates between the traffic from clients with the legitimate users (Human) and the malicious users (bots).

Admission control and congestion control: The admission control to reduce the number of concurrent clients served by the online service. Admission control works based on port hiding that renders the online service invisible to unauthorized clients by hiding the port number on which the service accepts incoming requests.

TMH (Trust Management Helmet): This mechanism used for differentiate right users and attackers. Servers should give priority to protecting the connectivity of good users during the application layer DDOS attacks instead of identifying all the attack requests.

Hybrid detection based on trust and information theory based metrics: Hybrid detection scheme based on the trust information and information theory based metrics. Trust value for each client is assigned by the server based on the access pattern of the client and is updated every time the client communicates with the server.

RESPONSE CRITERION OF DEFENSE MECHANISMS AGAINST FLOODING ATTACK

Before the attack (attack prevention): Attack prevention is held at the starting stage of the attack. Prevention mechanism performed at the source, destination, intermediate network.

System and protocol security mechanisms to increase the overall security of the systems: By preventing from unauthorized user to access the machine, removing bugs, updating installed protocols, installing software patches, removing unused software.

Fail-safe protection: Possible anticipations in case something goes wrong.

Resource allocation and accounting: User access the resources based on the privileges and the behavior.

Reconfiguration mechanisms: By tolerating the DDOS attack to change the topology of the target network.

Installing firewalls and improved intrusion detection and prevention systems: The destination host is installed by IDPS and it will prevent from the unauthorized user.

Employing local filters: It will block the attack before exploring the attack.

Load balancing and flow control: These two mechanisms are used for preventing from DDOS attack. It will improve the performance and mitigation of machine.

Server-side specific security considerations: The main problem of DDOS attack is to find out the server. Security policies are used to secure the server.

During the attack (attack detection): Detection techniques are performed during the attack. These techniques are focused at the source, destination, intermediate network and the combination of all. Anomalies pattern are identified in both Network Layer and Application Layer. MIB, MULTOPS, TOPS are the techniques which is used for detection.

After the attack (attack source identification and response): Defense system should use for after identifying the DDOS attack to block that attack.

Attack source identification: The attacker sends the message with the foged IP address to the victim. By using trace back mechanism to find out the original IP address with the help of reverse mechanism.

Initiating a proper response: After identifying the attack, initiate a response. For instance, history-based IP filtering, hop-count filtering, TRACK and StopIt, employ packet filtering upon detection of DDoS attacks and ACC, Pushback, PAD, AITF, DEFCOM are the some of the techniques.

CONCLUSION

DDoS attacks are created possible by natural faults in the world wide web style and the deficiency of appropriate protection systems in several pcs. The issue is only going to be created more serious later on. There are an incredible number pc systems being included to the world wide web every year. This can be sure that there are not going to be an incredible number of new system directors for these new serves. Many of these techniques will be used by home customers with long lasting IP details on a high speed internet relationship. This improves an already extremely focus on wealthy atmosphere for assailants to look for techniques that can be used as DDoS strike providers. It will also be challenging to collect useful forensic proof from techniques being run by people who might not even under take a position the idea of a TCP/IP stack, let alone collect useful forensic proof.

REFERENCES

Abadi, M., M. Burrows, M. Manasse and T. Wobber, 2003. Moderately hard, memory-bound functions. Proceeding of NDSS 2003 (Networks and Distributed Systems Security), pp: 25-39.

Abdelsayed, S., D. Glimsholt, C. Leckie, S. Ryan and S. Shami, 2003. An efficient filter for denial of service bandwidth attacks. Proceeding of the 46th IEEE Global Telecommunications Conference (GLOBECOM '03), 3: 1353-1357.

Bellovin, S., M. Leech and T. Taylor, 2001. ICMP Traceback Messages. Internet Draft, Work in Progress. Retrieved form: http://search.ietf.org/internet-drafts/draft-ietf-itrace-01.txt (Accessed on: October, 2001).

Carl, G., G. Kesidis, R.R. Brooks and S. Rai, 2006. Denial-of-service attack-detection techniques. IEEE Internet Comput., 10(1): 82-89.

Malan, G.R., D. Watson, F. Jahanian and P. Howell, 2000. Transport and application protocol scrubbing. Proceeding of INFOCOM 2000, pp: 1381-1390.

Palmieri, F., S. Ricciardi and U. Fiore, 2011. Evaluating network-based Dos attacks under the energy consumption perspective: New security issues in the coming green ICT area. Proceeding of the International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA, 2011), pp: 374-379.

Ricciardi, S., D. Careglio, U. Fiore, F. Palmieri, G. Santos-Boada and J. Solé-Pareta, 2011. Analyzing local strategies for energy-efficient networking. Proceeding of the SUNSET 2011, IFIP NETWORKING. Valencia, Spain, LNCS 6827, pp: 291-300.

Stephen, S. and L. Ruby, 2003. Taxonomies of Distributed Denial of Service Networks Attacks, Tools and Countermeasures. Retrieved form: http://www.ee.princeton.edu/~rblee/DdoS%20Survey%20Paper_v7final.doc.