The Distributed Denial of Service Attacks (DDoS) Prevention Mechanisms on Application Layer

Karuna S. Bhosale, Maria Nenova, Georgi Iliev

Abstract—**As DDOS attacks interrupt internet services, DDOS tools confirm the effectiveness of the current attack. DDOS attack and countermeasures continue to increase in number and complexity. In this paper, we explore the scope of the DDoS flooding attack problem and attempts to combat it. A contemporary escalation of application layer distributed denial of service attacks on the web services has quickly transferred the focus of the research community from conventional network based denial of service. As a result, new genres of attacks were explored like HTTP GET Flood, HTTP POST Flood, Slowloris, R-U-Dead –Yet (RUDY), DNS etc. Also after a brief introduction to DDOS attacks, we discuss the characteristics of newly proposed application layer distributed denial of service attacks and embellish their impact on modern web services**

Keywords- App-Ddos attacks, Http Get, Http Post, Slowloris, RUDY, DNS.

I. Introduction

The rapid development of Internet had resulted in the increase of online attacks. Among many, DDOS attack has evolved to be most powerful and harmful attack. A malicious software called 'Bots' is injected in computers to be compromised to perform specific and automated function. Bots, larger in number also called as 'Botnet' create prime crimes such as, widespread delivery of Spam emails, Click-fraud, spyware installation, virus and worm dissemination, DDOS attacks [1]. Such attacks infiltrate the networks bandwidth and also resources of victims, thus making smoother the denial of access to legitimate users.

A current, cosmopolitan and popular method of DDOS attack involves application level flooding, specifically the web server. Application layer distributed denial of service attacks, intends to disrupt application services rather than exhausting the network resources. A current, cosmopolitan and popular method of DDOS attack involves application level flooding, specifically the web server. Application layer distributed denial of service attacks, intends to disrupt application services rather than exhausting the network resources. Over the years it has emerged to be a larger threat on web services compared to typical denial of service. Various flooding methodologies are employed by DDOS such as HTTP GET Flood, HTTP POST Flood, Slowloris, and DNS etc. Fig. 1. Depicts the graphical distribution of DDOS attacks application layer, as reported by the Arbor, Inc. [2]. From Figure it is easily understood, that HTTP attacks are higher in percentage as compared to other attacks. HTTPs reach highest incidence of DDOS attacks reading up to 86% [2]. This graph highlights that, HTTP Flooding attacks are richly targeted.

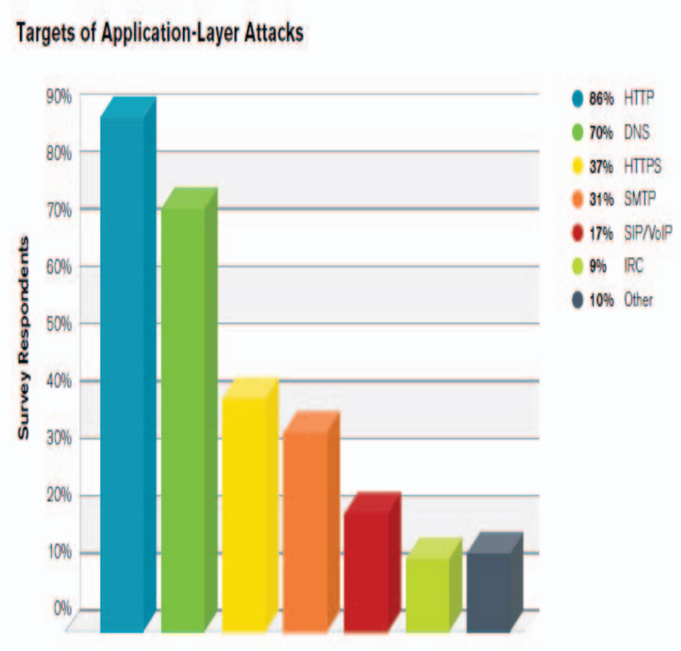

Fig.1 Types of DDoS attacks on the application layer.

II. DDOS Attacks and Countermeasures

DDoS Attacks Taxonomy:

Numerous DDOS attacks are observed. But two main classes of DDOS attack:

1) Bandwidth depletion : Bandwidth Depletion attack are categorized as follows:

a) Flood attacks: Flood attacks can be defined as to create a severe problem in infrastructure by overloading the traffic and also to assume available victim. Flood attacks intends in first

Karuna S. Bhosale is with the Faculty of Telecommunication, Technical University of Sofia, Sofia, Bulgaria, e-mail: bhosale.karuna@gmail.com

Maria Nenova and Georgi Iliev are with the Faculty of Telecommunication, Technical University of Sofia, Sofia, Bulgaria, e-mail: mvn@tu-sofia.bg, gli@tu-sofia.bg

978-1-5386-1800-4/17/$31.00 ©2017 European Union

occupying the host's resources and consumption of network bandwidth. If the malicious data is dominating, legitimate flow is blocked. Flood attack is categorized into protocol attack which takes advantage of Internet protocols.

b) Amplification attacks: To broadcast IP addresses in amplification attacks, attackers and zombies are involved. To decrease the victim systems bandwidth, broadcast IP address is used to amplify and reflect the attack traffic.

2) Resource depletion attack: It is of two type as follows:

a) Protocol exploit attacks: In a DDOS TCP SYN attack, the attacker instructs the zombies to send in order to link up with the resources in order to prevent the sever from replying to legitimate user's requests. The TCP SYN attack, by sending spoofed source IP addresses renders the three way handshake between the communicating systems.

b) Malformed Packet attacks: In such an attack, the zombies are instructed to send malicious i.e. incorrect form of IP packets to the victim system in order to crash the system. Malicious packets contain same source and destination IP address in order to confuse the operating system of victim. Such type of attack also causes delay and if attack is multiplied, it can exhaust the processing ability of the victim system [3].

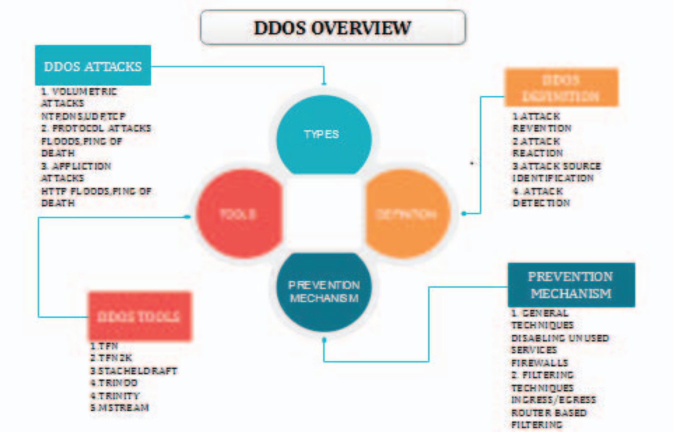

Fig. 2 DDOS Overview.

III. DDOS Attack Tools

The availability and effectiveness of the attacking tools for DDOS make the DDOS attack widespread. Some of the most common attacking tools are as follows:

i) Trinoo: It is used for a coordinated UDP flooding attack. It is used for deploying master/slave configuration and hence the attacker gain controls a number of Trinoo master machines. With the TCP and UDP protocols the communication between attacker and master and master and slave is established.

ii) TFN: This tool uses a command line interface to exhibit communication between attackers and control master without encryption between attacker and master or between and slaves. Communication is established via ICMP packets. This tool can implement smurf, SYN flood, UDP flood, and ICMP flood attacks.

iii) TFN2K: It is an advanced tool for TFN. It makes a combination of all, TCP, UDP and ICMP to establish communication between master and slave machines.

iv) TFN2K is helpful in implementing SYN, Smurf, UDP and ICMP flood attacks. Key based algorithm is used to make communication between real attacker and master.

v) Stacheldraht: This tool is combination of both Trinoo and TFN. It automatically updates slave machines. While communication between master control and attacker is through TCP and ICMP .SYN, UDP, Smurf and ICMP floods are implemented through Stacheldraht.

vi) Shaft: Apart from using port numbers for communication its working is similar to Trinoo. This tool is able to switch control between master servers and ports in real time hence making detection difficult. Shaft implements ICMP, UDP, and TCP flooding attack.

vii) Mstream: It is one of the primitive tool available. It attacks through a TCP ACK flood. A non-encrypted connection is made. One or more attacker using protected password control the masters. Masters are informed whether they are successfully accessed or not.

viii) Knight: Here, a control channel IRC is used. It can implement SYN attack, UDP flood attacks and an urgent pointer flooder. It has been designed in such a way so that it can run on windows systems. It is featured with automotive updates via http or Ftp, a checksum generator and more.

ix) Trinity: It is also called as IRC based DDOS tool. It is utilized in making TCP SYN, TCP RST, TCP ACK flooding attacks. A specific IRC channel is combined with trinity which waits for commands. As IRC service is used for communication between attacker and agents increases the level of Threat.

Classification of DDOS Prevention Mechanisms:

DDOS prevention mechanism can be broadly classified as:

A) General Techniques: These are common techniques like Protection of systems, replication of resources. General Techniques is further classified as follows:

1) Disabling Unused Services: In such service system should have less number of open ports and less application. Hence it has less vulnerability for attackers. Examples of such attack are UDP echo and Character generation services.
2) Install Latest Security Patches: Regularly the system has to be updated. Also removing known security holes and installing relevant security patches prevents the system from exploitation of vulnerabilities.
3) Disabling IP Broadcast: Use of Intermediate broadcasting nodes, e.g. ICMP flood attacks and smurf attacks will become successful if all the computers including host and neighboring network disable IP broadcast.
4) Firewalls: It is an effective method to avoid flooding type attack from system behind the firewall. Firewalls simply allow or deny protocols, ports or IP addresses.
5) Global Defense Infrastructure: In a given network, the most important router is installed by filtering rules. Hence any DDOS attack can be prevented from entering the system as it has to pass through such filtering rules.
6) IP Hopping: From the pool of similar servers or with a pre-specified set of IP address, DDOS attack can be

restricted by changing locator or IP address of the active server. Thus the IP address of the victim became invalid. But such process makes the system vulnerable.

B) Filtering Techniques: Filtering techniques is divided into Ingress and Egress filtering.

1) Ingress/Egress filtering: Ingress is inbound while egress is outbound. In Ingress filtering there is a restriction of dropping addresses which are not matched with the Domain Name attached to the ingress router. While egress is an outbound filtering only these packets will leave the network which have assigned and allocated IP address space for complicated networks, it is hard to obtain the assigned IP address space.

2) Router based packet Filtering: It is an extension of ingress filtering and with the help of route information, spoofed IP address is filtered out. But there are many limitations; first limitation is it relates to the implementation of RPF. The second is RPF drop legitimate packets if the route has been changed. Finally it is concluded that RPF is vulnerable to asymmetrical and dynamic Internet Routing.

3) History Based IP Filtering: During DOS attack, most of the source IP address is seen apart from those seems in normal operation. To search the source IP address, Hash or Bloom filters technique is used. Unfortunate History based IP filtering is ineffective, if the attacker is from real IP addresses.

4) Secure Overlay Service (SOS): It is defined as architecture, where the communication between confirmed user and victim is secured. All the traffic is verified and checked by SOS throughout the path. SOS is responsible to guarantee the communication between legitimate user and victim. The success of attack lies in breaching the security of SOS.

5) Source Address Validity Enforcement (SAVE): It is a protocol which enable filtering the packets with spoofed source address. It enables routers in updating the information of expected source IP address on each link while blocking IP Packet with unexpected source address. SAVE aims at giving the router the information regarding range of source IP address.

IV. Application Layer DDOS Attacks and Countermeasures

Application level DDOS flooding attacks, are intended to disrupt legitimate user's services by consuming server resources for ex., sockets, CPU, memory, disk/database, bandwidth and input/output bandwidth [1].As these attacks are popular for being stealthy and occupy less bandwidth, they are similar to benign traffic. Their impact is similar to as volumetric attacks as they target specific characteristics of application such as HTTP, DNS or SIP. Recently DDOS flooding attacks are considered as to be major types of attacks employing ddos attack are:

1) Reflection /Amplification based flooding attacks: Both reflection and amplification are employed by DNS amplification attack. Using fake source IP address large amount of DNS queries are generated as DNS response messages are larger than DNS query. Another example for amplification flooding is VOIP flooding.

2) HTTP flooding attacks: There are four types of attacks*:*

a) Session flooding attack:

b) Request Flooding attacks [4]

c) Asymmetric attacks:

i) Multiple HTTP GET/POST Flood

ii) Faulty Application

iii) Slow request/response attacks

iv) Slowloris attack

v) HTTP Fragmentation attack

vi) Slow post Attack

vii) R-U-Dead-Yet(RUDY)

Defense Mechanism against application Level DDOS Flooding Attack: It has following types:

1) Destination-based (server-side) mechanisms: Mostly client-server model are employed for application layer protocols. A server extracts the request made by client (DNS Server, Web server).such mechanism is deployed at destination attack. Some of major mechanism against such application level DDOS flooding attacks are as follows:

a) Defense against Reflection/Amplification attacks: This detection methods aims at detecting malicious traffic from different protocols such as DNS and SIP by employing various mechanism such as machine learning techniques. The proposed technique is DNS Amplification attacks Detector (DAAD) [5].

b) DDOS-Shield [6]: HTTP characteristics are detected by using statistical methods. DDOS shield consist of suspicious assignment mechanism and a DDOS resilient scheduler. It behaves as a rate limiter which utilizes continues values to decide when to use session values. Anomaly detector based on hidden semi-Markov model [7]: This method uses Hidden –markov model which describes dynamics of access matrix for detection of attacks.

c) DAT (Defense against Tilt DDoS attacks) [8]: The uses of features like instant traffic, volume, session behavior are monitored by DAT. For various users, DAT provides different services.

d) Hybrid (Distributed) mechanisms: Employing collaboration and cooperation between clients and server are mechanism of hybrid defense. They detect and respond to attacks. Some of mechanisms are as follows:

i) Speak-Up [9]: The goal of this method is to differentiate between good and bad clients, to capture a larger fraction of the server's resources. Speak Up method is applicable against session flooding attacks.

ii) DOW (Defense and Offense Wall) [10]: K-Means clustering method is used to detect and filter session attacks, request flooding attacks and asymmetric attacks.

iii) Differentiate DDoS flooding bots from human [11]: This

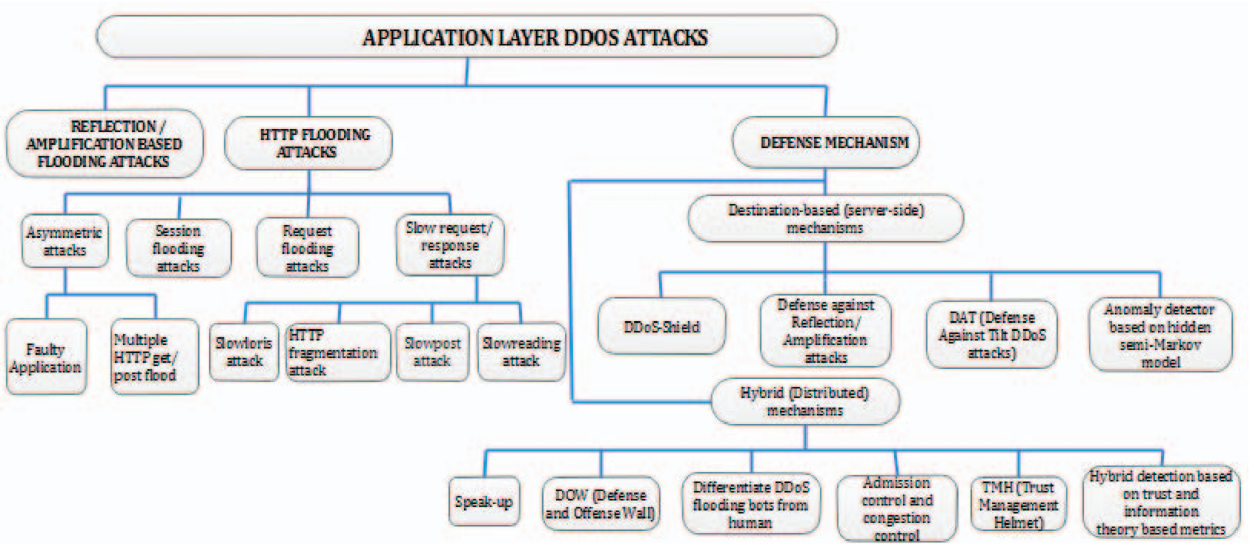
APPLICATION LAYER DDOS ATTACKS
REFLECTION / AMPLIFICATION BASED FLOODING ATTACKS
HTTP FLOODING ATTACKS
DEFENSE MECHANISM
Asymmetric attacks
Session flooding attacks
Request flooding attacks
Slow request/ response attacks
Faulty Application
Multiple HTTP get/ post flood
Slowloris attack
HTTP fragmentation attack
Slowpost attack
Slowreading attack
Destination-based (server-side) mechanisms
DDoS-Shield
Defense against Reflection/ Amplification attacks
DAT (Defense Against Tilt DDoS attacks)
Anomaly detector based on hidden semi-Markov model
Hybrid (Distributed) mechanisms
Speak-up
DOW (Defense and Offense Wall)
Differentiate DDoS flooding bots from human
Admission control and congestion control
TMH (Trust Management Helmet)
Hybrid detection based on trust and information theory based metrics

Fig. 3. Application layer ddos flooding attacks types and defense mechanism.

mechanism differentiate between legitimate users (human) and malicious users (bots). Hence systems called completely Automated Public Turing Test to Tell computers and Humans Apart (CAPTCHA) is employed.

iv) Admission Control and Congestion Control [12]: Admission control is employed to limit the number of concurrent clients. Admission control is based on port hiding and renders online services.

v) TMH (Trust Management Helmet) [13]: Trust management is employed to differentiate between legitimate users and attackers. The intention of TMH is that the servers should prior protect the connectivity of authentic users during attack.

Hybrid detection based on trust and information theory based metrics [14]: This mechanism firstly filter out suspicious flows based on the trust value. Web user browsing behavior (HTTP Request rate, page viewing time) are based on entropy.

V. Conclusion

In this paper, is explored the scope of the DDoS flooding attack problem and different types of technical attempts to combat it. The focus is based on the analysis of characteristics of newly proposed application layer distributed denial of service attacks. The impact of this type of attack was also presented. DDoS flooding attacks specific characteristics and defense mechanism were also investigated focus is based on the analysis of characteristics of newly proposed application layer distributed denial of service attacks. The impact of this type of attack was also presented. DDoS flooding attacks specific characteristics and defense mechanism were also investigated.

References

[1] Esraa Alomari, 2Selvakumar Manickam, 3,4B. B. Gupta, 5Shankar Karuppayah, 6Rafeef Alfaris, "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

[2] D McPherson, R Dobbins, M Hollyman, C Labovitzh, Worldwide infrastructure security report, Volume v, Arbor Networks, 2010

[3] Ryotaro Kobayashi,Genki Otami,Takuro Yoshida,Masafiko Kato, "Defense Method of HTTP GET Flood attack by adaptively controlling server resources depending on different Attack", Journal of Information Processing vol.24(802-815)september 2016.

[4] Saman Taghavi Zargar, Member, James Joshi, Member, and David Tipper, Senior Member, A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE communications surveys & tutorials, accepted for publication, published online Feb. 2013.

[5] G Kambourakis, T Moschos, D Geneiatakis, "detecting dns amplification attacks" CRITIS 2007, LNCS 5141, pp. 185–196, 2008. © Springer-

[6] S Ranjan, R Swaminathan, M Uysal, A Nucci, "DDoS-shield: DDoS-resilient scheduling to counter application layer attacks", IEEE/ACM Trans. Netw., Vol. 17, no. 1, pp. 26-39, February 2009

[7] Yi Xie and Shun-Zheng Yu, Member, "A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors" IEEE/ACM transactions on networking, vol. 17, no. 1, february 2009

[8] HI Liu, KC Chang, "Defending systems Against Tilt DDoS attacks" Telecommunication Systems, Services, and Applications (TSSA), pp. 22-27, October 20-21, 2011

[9] Michael Walfish, Mythili Vutukuru, Hari Balakrishnan, David Karger , and Scott Shenker," DDoS Defense by Offense", SIGCOMM '06, September 11–15, 2006

[10] Jie Yu 1 , Zhoujun Li 2, Huowang Chen 1 , Xiaoming Chen 2, "A Detection and Offense Mechanism to Defend Against Application Layer DDoS Attacks", third International Conference on Networking and Services (ICNS'07), pp. 54, June 19-25, 2007.

[11] S Kandula, D Katabi, M Jacob, A Berger, "Botz-4-sale: Surviving organized ddos attacks that mimic flash crowds", Proc. of Symposium on Networked Systems Design and Implementation (NSDI), Boston, May 2005.

[12] Mudhakar Srivatsa, Aun Iyengar, and Jian Yin, "Mitigating Application-Level Denial of Service Attacks on Web Servers: A Client-Transparent Approach" ACM Transactions on the Web, Vol. 2, No. 3, Article 15, Publication date: July 2008

[13] Jie Yu, Chengfang Fang†, Liming Lu, Zhoujun Li, "A Lightweight Mechanism to Mitigate Application Layer DDoS Attacks", Proc. of Infoscale 2009, LNICST 18, pp. 175191, 2009

[14] S. Renuka Devi and P. Yogesh, "A Hybrid Approach to Counter Application Layer DDOS Attacks" International Journal on Cryptography and Information Security (IJCIS), Vol.2, No.2, June 2012.