A SURVEY OF TRENDS IN MASSIVE DDOS ATTACKS AND CLOUD-BASED MITIGATIONS

FuiFui Wong and Cheng Xiang Tan

Department of Computer Science and Technology, TongJi University, Shanghai, 201804, China

ABSTRACT

Distributed Denial of Service (DDoS) attacks today have been amplified into gigabits volume with broadband Internet access; at the same time, the use of more powerful botnets and common DDoS mitigation and protection solutions implemented in small and large organizations' networks and servers are no longer effective. Our survey provides an in-depth study on the current largest DNS reflection attack with more than 300 Gbps on Spamhaus.org. We have reviewed and analysed the current most popular DDoS attack types that are launched by the hacktivists. Lastly, effective cloud-based DDoS mitigation and protection techniques proposed by both academic researchers and large commercial cloud-based DDoS service providers are discussed.

KEYWORDS

DoS, DDoS, DNS reflection or amplification attack, SYN flood, UDP flood, ICMP flood, HTTP flood attack

1. INTRODUCTION

In March, 2013, Spamhaus.org was suffering the largest distributed denial of service (DDoS) attacks on record, with an estimated size of more than 300 Gbps [1]. CloudFlare with cloud-based DDoS protection solutions was engaged to mitigate this attack. According to Prolexic's Q1 2013 Global DDoS Attack Report, more than 10% of the massive DDoS attacks today have exceeded 60 Gbps, and more than 75% of the attacks are directed to infrastructure (Layer 3 and 4), against bandwidth capacity and routing infrastructure; the remaining attacks are on the application layer [2].

In a DDoS attack, the attackers attempt to temporarily interrupt or suspend the services of a website so that it is unavailable to the users. Akamai's Fourth Quarter, 2012 State of the Internet Report has stated that a total of 768 DDoS attacks were reported in 2012. Over a third (269 or 35%) of the attacks targeted companies in the Commerce sector, 164 attacks (22%) targeted Media and Entertainment companies, 155 attacks (20%) targeted Enterprise companies that include financial services, 110 attacks (14%) targeted High Tech companies, and 70 attacks (9%) targeted Public Sector agencies [3]. These attacks have cost targeted companies or organizations losses in revenues, customer satisfaction and brand equity.

This survey aims to provide a complete update on the current most popular DDoS attack types used in massive attacks and to discuss the various effective cloud-based DDOS mitigation and protection techniques. In Section 2 of the survey, we first look into the current largest DDoS attack on Spamhaus in detail. We then discuss the current most popular infrastructure (layer 3 and 4) and application layer attack types in Section 3. Various effective cloud-based DDOS mitigation

DOI : 10.5121/ijnsa.2014.6305

and protection techniques are discussed in Section 4, and lastly, we present our conclusions in Section 5.

2. HISTORIC DDOS ATTACK ON SPAMHAUS

On 18 March, 2013, spamhaus.org, a website of Spamhaus that provides anti-spam filtering services online, was attacked by a massive DDoS that was more than 100 Gbps. This attack was enormous and saturated their Internet connection; access to their website was not possible. The attacks were classified as Layer 3 attacks and were difficult to resolve with a software solution because the router was saturated with excess network traffic compared with the traffic that it can handle. The identity of the attacker was unknown during that time.

These large Layer 3 attacks are from many sources and are distributed, whereby sources send traffic to flood the targeted Internet location. A group of individuals working together, a botnet of compromised PCs, a botnet of compromised servers, misconfigured DNS resolvers, or even home Internet routers with weak passwords could be the sources of attack traffic.

DDoS prevention techniques such as IP filtering will not be effective anymore because a Layer 3 attack is launched by sending randomised packets that contain spoof information, including the source IP, and the received responses will be ignored. CloudFlare, a company that offers cloud-based DDoS protection solutions, was engaged by Spamhaus to mitigate the attack, and the site was up within hours [1].

2.1 Generation of the 75 Gbps DDoS Attack to Spamhaus

Since 2012, DNS reflection attack has become the main source of the largest Layer 3 DDoS attacks. The largest attack traffic for Spamhaus was from DNS reflection.

The attacker of Spamhaus began by requesting a DNS zone file for ripe.net from the open DNS resolvers. The CloudFlare IPs assigned to Spamhaus were spoofed by the attacker in their DNS requests. The DNS zone file responded by opening resolvers that generated approximately 75 Gbps of attack traffic, which resulted from an amplified 36-byte request to a 3,000-byte response.

30,000 unique DNS resolvers were involved in the Spamhaus attack. Each open DNS resolver was sending a 2.5 Mbps DNS zone file, which was allowed by most DNS resolvers. The attacker then used only DNS amplification and controlling a botnet or cluster of servers to generate a 750 Mbps DNS zone file.

2.2 Mitigation of the 75 Gbps DDoS Attack to Spamhaus

Anycast was used by CloudFlare to mitigate the 75 Gbps DDoS attack on Spamhaus. Anycast scatters an attack on Spamhaus to the 23 worldwide data centers of CloudFlare. Every data centre used the same IP address for Spamhaus, which had the result that the traffic could not be targeted to any one location. Instead of a many-to-one attack, the attack becomes many-to-many and unable to cause a bottleneck at any single point in the network. After the attack was scattered, the Layer 3 attack was stopped at each of the CloudFlare data centers before reaching Spamhaus servers.

3. CURRENT UPTREND OF MASSIVE DDOS ATTACK TYPES

The Open Systems Interconnection (OSI) model divides a communication system into seven logical layers. Each layer has its own unique security challenges and is vulnerable for the Denial of Service (DOS) attack or Distributed Denial of Service (DDoS) attack. The uptrend of Distributed Denial of services attacks for the last two years primarily fall into two categories of attack: Infrastructure (Layer 3 & 4) attacks and Application (Layer 7) attacks. Attacks in the first category, infrastructure attacks, attempt to overwhelm the bandwidth capacity and routing infrastructure by sending very large number of spurious requests. The second category, application attacks, exploits the limitation of a specific application to cause performance degradation or ultimately crashing the remote servers.

3.1 Infrastructure (Layer 3 and 4) Attacks

This section describes the current most popular DDoS attack types on the network layer (Layer 3) and transport layer (Layer 4) in the OSI model, which are the following:

- DNS Reflection Attacks
- TCP SYN floods
- UDP floods
- ICMP floods

Based on the statistical record published on the security reports by the well-established leading industries [2-4], these attack types are the primary focus of malicious actors and will stay at the top on the global threatscape.

3.1.1. Domain Name Server (DNS) Reflection or Amplification Attacks.

A DNS Reflection or Amplification attack is a type of distributed denial of service (DDoS) attack in which an attacker sends a DNS name lookup request to an open DNS resolver with the source address spoofed to be the victim's address. When the DNS server sends the DNS record response, it is sent to the victim (the source address that was used in the spoofed request). Because the size of the response is typically considerably to be larger than the request, the attacker can amplify the volume of traffic directed at the victim. By leveraging a botnet to perform additional spoofed DNS queries, an attacker can produce an overwhelming amount of traffic with very little effort, as shown in Figure 1. Because the responses are legitimate data coming from valid name servers, it is especially difficult to block these types of attacks [5].

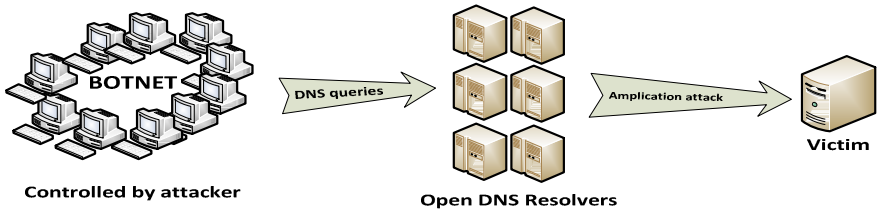

Fig. 1 DNS Reflection Attack

A DNS Reflection attack is made possible by the following [6]:

Open recursion. Open DNS resolvers are referred to as servers on the Internet and have recursion enabled, and they provide recursive DNS responses to anyone. According to Open Resolver Project, there are approximately 27 million open DNS resolvers currently on the

Internet. Open DNS resolvers are the source of amplification, returning a much larger DNS response after receiving a small DNS query.

Source address spoofing. A DNS amplification attack is similar to a "Smurf" attack, in which the source address for the DNS query is spoofed with a return address other than the sender's. Then, an open resolver returns a DNS response that is incorrectly sent to the spoofed address [7].

Botnets. In a DNS amplification attack, the attacker has compromised groups of online computers that are known as Botnets for sending DNS queries to open resolvers.

Malware. DNS amplification attacks are triggered by botnet computers infected with Malware.
EDNS0. A 64-byte query will result in an 8x amplified 512 byte UDP reply if it is without Extension Mechanisms for DNS (EDNS0) [8], allowing DNS requestors to advertise their UDP packets size and facilitate the transfer of packets larger than 512 bytes.

DNSSEC. DNSSEC (short for DNS Security Extensions) [9] allows DNS servers to validate DNS responses and prevents cache-poisoning attacks with cryptographic signatures added, resulting in a larger DNS message size that requires EDNS0 support. DNSSEC has been criticised for contributing to DNS amplification attacks because a server that supports DNSSEC will also support large UDP packets in a DNS response.

3.1.2. TCP SYN Floods.

SYN flooding attack works on the design of a 3-way handshake to begin a TCP connection. In this handshake, as shown in Figure 2, the client system begins by sending a SYN message to the server. The server then acknowledges the SYN message by sending a SYN-ACK message to the client. The client then finishes establishing the connection by responding with an ACK message. The connection between the client and the server is then open, and the service-specific data can be exchanged between the client and the server. The potential for abuse arises at the point where the server system has sent an acknowledgment (SYN-ACK) back to the client but has not yet received the ACK message [10].

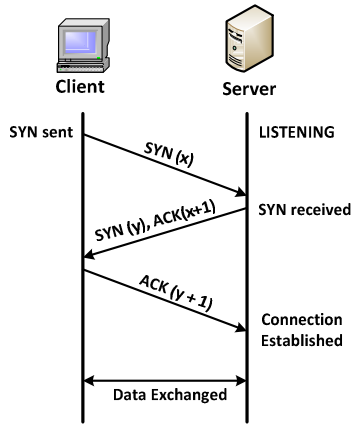

Fig. 2 TCP 3-way handshake

The Transmission Control Block (TCB), a transport protocol data structure that holds all of the information on a connection, is allocated, and the connection is only half open after the SYN packet has been received by the server before the ACK message is received from the client. This situation leads to the server's kernel memory being exhausted by incoming SYNs, which create too many TCB allocations. However, Operating systems will usually use a "backlog" parameter with a listening socket to avoid this memory exhaustion, but depleting the backlog is the goal of the TCP SYN flooding attack, which attempts to send enough SYN segments to fill the entire

backlog and, thus, causes the service to be denied to the new connection requests. Figure 3 below presents a simplification of the sequence of events that are involved in a TCP SYN flooding attack.

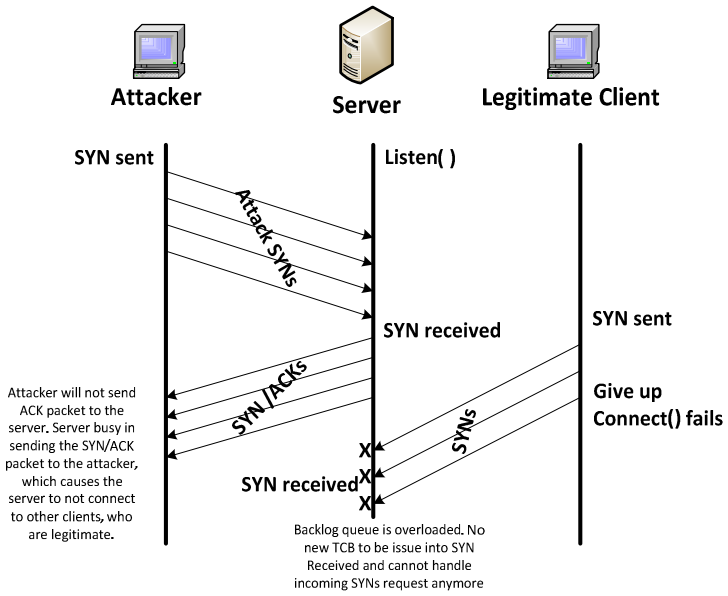

Fig. 3 TCP SYN flooding attack

Currently, there are 3 variants of TCP SYN flooding attacks [11] found on the Internet:

i) Direct Attack. A direct attack is where the attackers send many SYN segments without spoofing their IP source address, and they prevent their operating system from responding to the SYN-ACKs. This scenario can be accomplished through firewall rules that either filter outgoing packets to the listener (allowing only SYNs out) or filter incoming packets so that any SYN-ACKs are discarded before reaching the local TCP processing code, as shown in Figure 4.

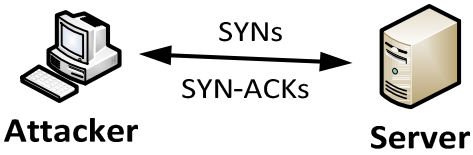

Fig. 4 Direct Attack

ii) Spoofing-Based Attacks. SYN flooding attacks [12] *use IP address spoofing, where the client systems at the spoofed source addresses are not responding to the SYN-ACKs sent to them, either because no client system exists at the address presently or because of the assumption that some percentage of the spoofed addresses will not respond,* as shown in Figure 5.

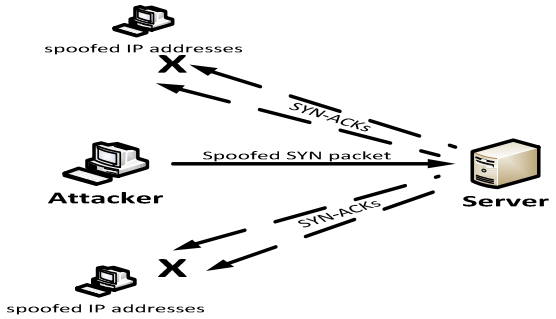

Fig. 5 Spoofing-based attacks

iii) Distributed Attacks. A distributed SYN flooding attack occurs when the attacker takes advantage of many drone machines or botnets throughout the Internet, and each changeable drone uses a spoofing attack and multiple spoofed addresses, which make the attack much more difficult to be blocked or stopped, *as shown in Figure 6*.

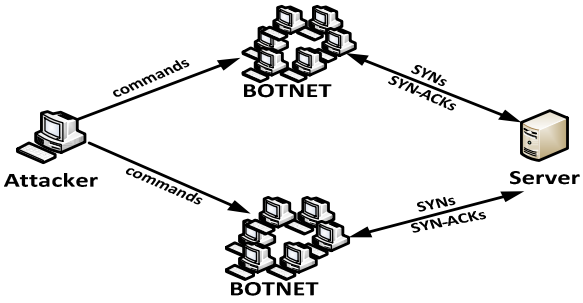

Fig. 6 Distributed attacks

3.1.3. UDP Floods.

A UDP flood is a type of bandwidth attack that uses the User Datagram Protocol (UDP). The UDP is a stateless transmission protocol that does not require the client and server to have an established session, and it has an emphasis on minimal latency rather than reliability in transmitting information. A UDP flood attack can be initiated by generating massive amounts of UDP packets to a random port on the victim system. The victim system will determine which application is waiting on the destination port in response to an incoming UDP packet. When the victim system that implements these services responds, it will respond to each UDP packet with an IMCP unreachable message to the forged source IP address if no application is waiting on the port. In this case, the malicious UDP sender forges the IP source address to be that of a victim, and thus, the victim's system is subject to being overloaded by the multiple UDP traffic responders. This type of attack most commonly exploits both the "chargen" and "echo" services weaknesses, as illustrated in figure 7, making them useful to the DoS attack (e.g., a UDP packet is composed of a source port of echo for the target host B and a destination port of chargen for the target host A) [13]. The chargen service will continue generating some random characters and send them back to the apparent source, whereas the echo service keeps continuing to respond to the packet by echoing the random characters back to the chargen. The attacker can pipe output from the chargen to echo and cause an infinite ending stream of network activity. This scenario creates an infinite loop between two UDP services, where host B will echo a packet to host A. Host A then responds to host B's echo port until the exhaustion of some shared resource (e.g., buffers, link, capacity) [14].

Because UDP is an unreliable protocol that does not regulate its sending traffic rate, this scenario can easily allow a malicious UDP sender to forge the IP source address to be that of a victim.

Most UDP floods are used frequently for the larger bandwidth DDoS attacks that are greater than 1 Gbps because it is easy to generate UPD packets from many different scripting and compiled languages [15].

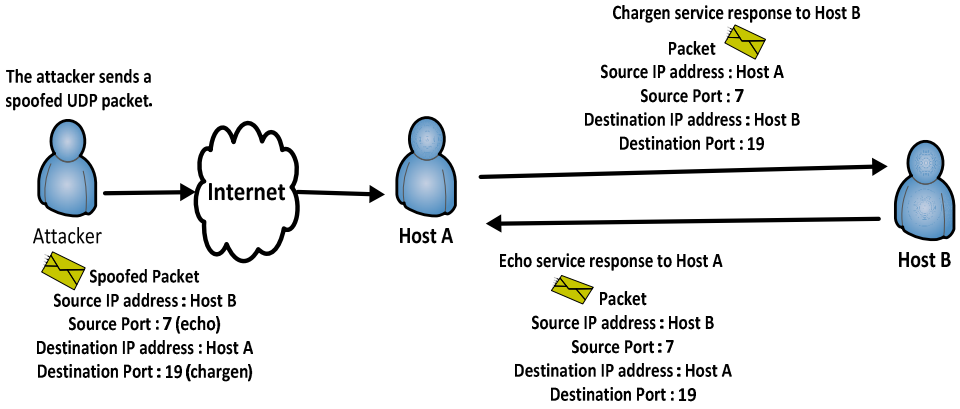

Fig. 7 UDP flooding attack

3.1.4. ICMP Floods.

The ICMP flood, occasionally referred to as a "Smurf" attack or "Ping" flood, is a ping-based DOS attack that sends large numbers of ICMP packets to a server and attempts to crash the TCP/IP stack on the server and cause it to stop responding to the incoming TCP/IP requests. Then, hping or custom perl scripts installed on the compromised machines are used to launch ICMP floods. Basic SYN floods are occasionally launched together with ICMP floods [2].
A SMURF attack occurs when an attacker sends ICMP requests with a victim's spoofed IP to the network's broadcast address of a router that is configured to relay ICMP to all of the devices behind the router. The attack is amplified when all of those devices respond back to the ping, where ICMP does not include a handshake and the source IP will not be verified. Figure 8 below presented a SMURF attack [16]. Please refer to [17] and [18] for a more detailed description of a Smurf attack.

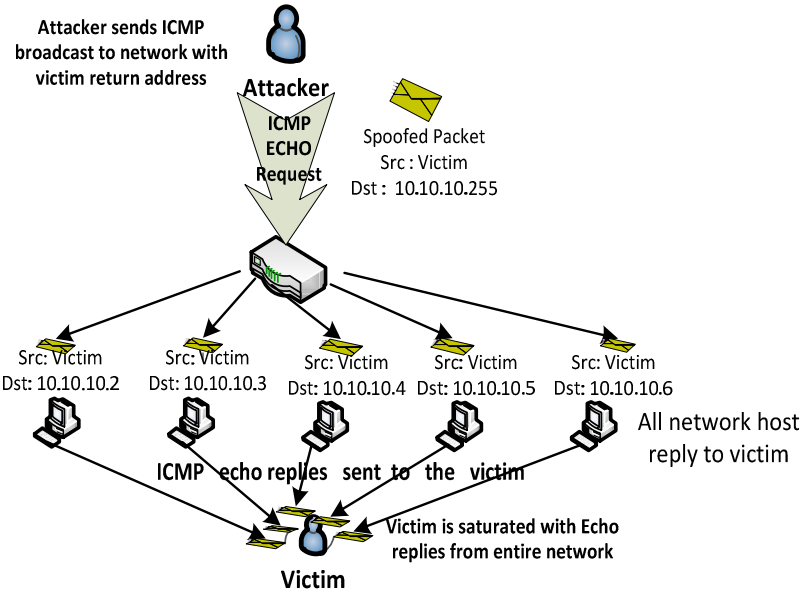

Fig. 8 ICMP flooding attack

3.2 Application (Layer 7) Attacks

The application layer DDoS attacks continue to grow in both complexity and prevalence. The research firm Gartner forecasts that 25% of the DDoS attacks in the year 2013 will be application-based, in the report titled, "Arming Financial and E-commerce Services Against Top 2013 Cyberthreats" [19]. DDoS attacks in the application layer attempt to target a specific service with a web flood; for example, HTTP flood attacks send high rates of legitimate application-layer requests to a server in an attempt to overwhelm the server resources. These attacks generally consume less bandwidth and are far more difficult to identify because the attacker attacks the victim server through a flood of legitimate requests [20].

3.2.1. Common Application-Layer DDoS Attack Types.

Application-layer attacks can be subdivided into four categories [21] [22]:

i) Request-Flooding Attacks occur when heavy legitimate application-layer requests (e.g., HTTP GETs, DNS queries and SIP INVITEs) are sent to a server to overwhelm its session resources.
ii) *Asymmetric Attacks* occur when normal requests that consume large amounts of server resources, such as CPU, memory or disk space, are sent to the web server with the objective of severely degrading its service or bringing the server completely down.
iii) *Repeated One-Shot Attacks* occur when a high workload request across many TCP sessions is sent to the server, with the goal of degrading or bringing down the service of the server. These attacks are similar to executing both request-flooding and asymmetric application-layer attacks.
iv) *Application-Exploit Attacks* target vulnerabilities in applications by causing a fault in a server's operating system or applications and allow the attacker to gain control of the application, system or network. Scripting vulnerabilities, buffer overflows, cookie poisoning, hidden field manipulation, cross-site scripting and Structured Query Language (SQL) injection are the examples of these attacks [23].

3.2.2. HTTP Flood Attacks.

According to Prolexic's Q1 2013 Global DDoS Attack Report, 23.46 per cent of the Total DDOS attacks come in application (layer 7) attacks, and 19.33 per cent of the total DDOS attacks come in the form of HTTP GET floods, which represent the majority of application attacks. Http Post floods, which enable attackers to POST large amounts of data to applications, are the second most popular of the application attacks, which make up 1.43 per cent of the total DDoS attacks [2].

There are 3 types of HTTP floods that can be launched, as follows [21]:

i) *HTTP Malformed Attacks* occur when invalid HTTP packets are sent to web servers to exhaust the server resources. An example of this type of attack, which uses malformed HTTP GET requests, is Zafi.B worm.
ii) *HTTP Request Attacks* occur when different types of legitimate HTTP requests (i.e., HTTP GETS, and POSTS) are sent to web servers in an attempt to flood them by consuming the server resources [24].
iii) *HTTP Idle Attacks* occur when HTTP connections are opened and left idle without actually sending a complete HTTP request by an attack. An example of this attack is "slowloris" [25], which involves indefinitely dribbling out a small number of bytes per packet to keep the connection from timing out but which never manages to complete the request .

4. CURRENT DDOS MITIGATION AND PROTECTION TECHNIQUES USED WITH THE CLOUD

Currently, common DDoS mitigation and protection techniques that are implemented on the small and large organizations' networks and servers find it difficult or no longer possible to mitigate the overwhelming gigabit attacks. Cloud computing with geographically distributed high Internet bandwidth and high processing power is required for these DDoS mitigation and protection techniques to be effective.

Various effective massive DDoS mitigation and protection techniques, which are researched by academic researchers and used by large commercial cloud-based DDoS service providers such as Prolexic, CloudFlare, Cisco, Akamai and Arbor for mitigating the attack types mentioned in the above section, will be discussed, as follows:

4.1 DNS Reflection or Amplification Attacks

4.1.1. Ingress filtering.

Ingress filtering checks the validity of the IP addresses that belong to your network for all of the outgoing packets and is fully written down in a Best Common Practices document, BCP-38. The DNS server reflects traffic that relies on spoofed IP addresses, which are dropped by using this filtering, and it is easy to implement in routers because all of the major router vendors have methods that are built-in, to implement BCP-38 [26].

4.1.2. Limiting DNS recursion.

Limiting DNS recursion [5] can be performed by:

i) Configuring your server to allow recursion for a list of authorised DNS servers
ii) Configuring firewall to block the DNS queries that are not coming from your designated internal recursive DNS servers.
iii) Configuring your server to use the recursive DNS servers of your ISP and then only allow the DNS queries that are related to these servers.
iv) Splitting your authoritative and recursive DNS servers so that the recursive DNS is reachable only from within the LAN, as in Figure 9 below.

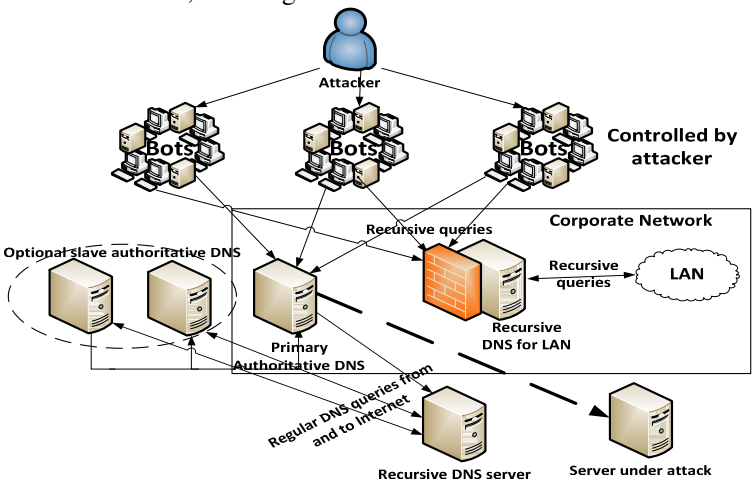

Fig. 9 Splitting Authoritative and Recursive DNS Servers

v) Using a hidden master so that only your slave authoritative DNS servers are publicly available on the Internet, as in Figure 10 below.

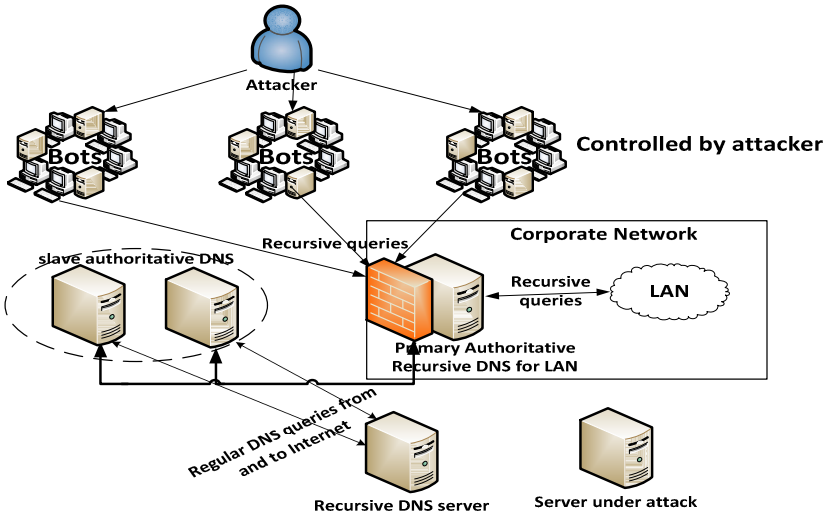

Fig. 10 Authoritative DNS is hidden master

4.1.3. DNS Response Rate Limiting.

DNS-RRL.DNS Response Rate Limiting is an experimental mechanism for limiting the number of responses per second returned by a DNS server. The effectiveness of a DNS amplification attack can then be reduced by dropping responses that exceed the configured rate limit. There are 3 ways that response rate limiting can be applied to a DNS server: by a source IP address, by a destination IP address and by the DNS query type [27].

4.1.4. Anycast.

Anycast allows multiple, identical, globally deployed DNS servers to advertise the same IP address. Using Anycast, each DNS server IP corresponds to hundreds of systems world-wide that are announced from different geographical locations. DNS servers reflect traffic that has spoofed IP addresses is then dropped at the closest DNS server to the querying client.

Most of the Anycast implementations are in the network layer, but research performed by the authors, Ioannis Avramopoulos and Martin Suchara, has proved that Anycast can be implemented in an applications layer, and the result shown is that the security performance is approximately the same as the network-layer implementation [28].

4.2 TCP SYN Flooding

SYN flooding mitigations have evolved into 2 classes, which are End-Host and Network based. End-Host mitigations involve hardening the end-host TCP implementation, which includes altering the algorithms and data structures that are used for connection lookup and establishment. Network-Based mitigations involve hardening the network, which either lessens the likelihood of the attack preconditions or inserts middleboxes that can isolate servers on the networks behind them from illegitimate SYNs [11].

End-Host mitigation techniques include the following:

i) Increasing TCP Backlog
ii) Reducing the SYN-RECEIVED Timer
iii) SYN caches and SYN cookies that operate by reducing the amount of state (SYN caches) / generating zero state (SYN cookies) that is allocated initially for a TCB generated by a received SYN, and putting off instantiating the full state.
iv) A hybrid approach that combines two or more of the above techniques.

Network-Based mitigation techniques include:
i) Ingress filtering that is very effective at preventing SYN flooding attacks, which rely on spoofed IP packets.
ii) Use firewalls and proxies to buffer end hosts from SYN flooding attacks through either spoofing SYN-ACKs to the initiators or spoofing ACKs to the listener.
iii) Use of a less expensive and easy-to-deploy active monitor device to observe and inject traffic to the listeners of the entire network without requiring every listener's operating system to implement an end-host mitigation.

Both End-Host and Network-Based mitigations are frequently employed and usually do not interfere when used in combination. Mitigations at End-Host are to take precedence over Network-Based because SYN flooding is targeted at end hosts rather than attempting to exhaust the network capacity.

The SYN caches technique is currently the most effective and most-often used end-host mitigation; it can withstand heavy attacks without the negative effects of SYN cookies, and heuristics for the threshold settings are not needed when they are employed in many hybrid approaches.

For Network-based mitigations, both SYN-ACK spoofing and ACK-spoofing of firewall/proxies produced the same effectiveness; active monitors are preferred to firewall/proxies for their low cost and easy administration, and both Ingress and egress filtering are commonly used as a good Internet security practice.

4.3 UDP Flood

The UDP flood attack has become prominent due to the recent high-profile attacks launched by a group of Internet activists called Anonymous [29, 30]. A DoS attack tool called LOIC (Low Orbit Ion Cannon), which performs flooding attacks using UDP packets, is widely available on the web. To mitigate the impact of UDP flooding attacks, several approaches have been proposed to suppress these types of attacks, such as prohibiting the UDP service, rate limits on UDP traffic, protection of proxy servers, and configuring the router to stop IP directed-broadcast transmission. For example, Komatsu et al. [31] have conducted a simulation that uses CHOKe with ACC (complex bandwidth control) as a congestion control method to prove the effectiveness of rate-limiting methods in mitigating UDP flood attacks.

4.4 ICMP Flood

ICMP flood attacks are losing popularity in the last few quarters, as stated in the Prolexic's Q1 2013 report. They are succeeded by more effective and stealthy attack methods that are available in the Internet. Currently, these attacks, which rely on the router serving a large multi-access broadcast network to frame an IP broadcast address, are easy to stop where the network operators deny the forwarding ICMP requests to a network's broadcast address by configuring their routers.

There are some operating systems that allow configurations for preventing your server from being used as an intermediary and that respond to the ICMP packets (which do not travel through a router on the local network) forwarded to an IP broadcast [17].

4.5 HTTP Flood Attacks

Vulnerability in the protocol is the main reason for flood attacks. A mitigation method for the flood attacks must consider the perspective of the system/protocol design to ensure an effective and successful implementation.

The HTTP protocol that serves at the application layer is used to launch HTTP flood attacks and can be detected and analysed by application layer security devices such as IPS (Intrusion Detection System) or WAF (Web Application Firewall). For other security devices at different layers of the OSI model, TCP connection counts made for the HTTP responses are the only detection method for them to prevent and block the HTTP Flood attacks.

The HTTP flood attacks can be mitigated at 5 main levels, as shown in Figure 11, which are the Cloud Services Level, Network Level, Web Server Level, Web Service Level, and Web Application Level [32]:

The Cloud Services Level and Network Level are the most important levels for detecting and blocking the HTTP flood attacks before reaching the web server.

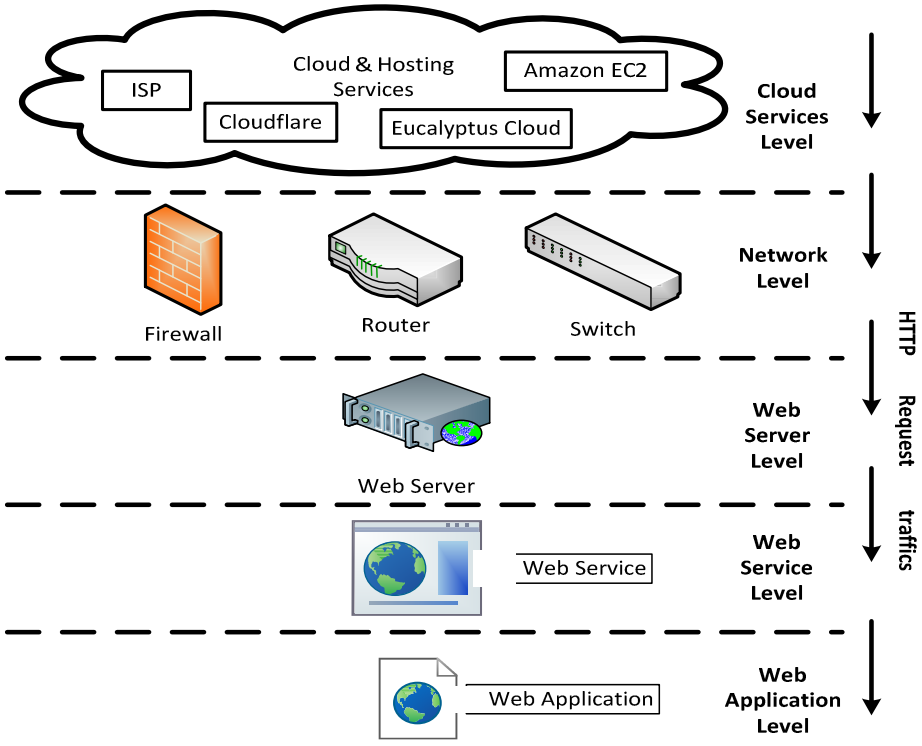

Fig. 11 Mitigation levels of HTTP flooding attack

4.5.1. IOSEC HTTP Anti Flood/DoS Security Gateway Module.

The author Gokhan Muharremoglu [32] has proposed a web application level approach against the HTTP Flood Attacks, IOSEC HTTP Anti Flood/DoS Security Gateway Module. This approach can be summarised into the following 3 steps:

i) Detect IP addresses of the abnormally excessive requests according to a previously defined rule,
ii) To reduce the attack surface, return the requests with a response that uses a small amount of resources (e.g., a blank page),
iii) Block detected IP addresses using other components at the other mitigation levels (e.g., WAF, web server/service).

Interested readers can refer to [32] for a more detailed description of the IOSEC HTTP Anti - Flood/DoS Security Gateway Module.

4.5.2. Detection of HTTP-GET Attack with Clustering and Information Theoretic Measurements.

The authors Chwalinski et al. [33] have recently proposed an off-line clustering technique that uses entropy-based clustering and the application of information-theoretical measurements to distinguish more than 80% of the legitimate and attacking sequences, regardless of the strategies chosen by the HTTP Flooding attackers.

The authors focus their research on the recent behaviour of actual web users by analysing the actual sequences of the web requests that the attackers do not know and could not reproduce. Two types of attacking hosts, frequently-changing and rarely-changing, are targeted by the proposed technique.

4.5.3. Detection of HTTP GET flooding attack in three different attack scenarios.

The authors Das et al. [34] have proposed a detection method for HTTP GET flooding attacks in three different scenarios, which are named in the following way:

i) Random Flooding App-DoS, which compares HTTP request arrivals with input thresholds.
ii) Shrew Flooding App-DoS, which detects the attacks using the generation of Legitimate Access Pattern (LAP) and computation of Pattern Disagreement (PD)
iii) Flash Crowds App-DoS, which uses a detection mechanism called DSB to perform offline analysis of attack datasets.

4.5.4. Arbor's Peakflow SP and Peakflow SP TMS to Stop Application-Layer DDoS Attacks.

Peakflow SP and Peakflow SP TMS are the commercial solutions that are provided by Arbor to stop DDoS attacks on the application layer. Peakflow SP is a very popular and effective DDoS mitigation solution that is capable of detecting bandwidth-consuming, connection-layer exhaustion and application attacks. The solution is used by the majority of the world's Internet service providers as one of their main DDoS detection and surgical mitigations.

Arbor relies mainly on a Peakflow SP Threat Management System (TMS) in their Peakflow SP solution to detect and mitigate HTTP flood attacks. This approach is a robust application-intelligent system for multi-service converged networks that speeds remediation by coupling high-level threat identification with packet-level analysis. It also provides visibility into critical

applications that are running on the network, and it can monitor key application performance metrics [21].

5. CONCLUSIONS

This study has presented a comprehensive survey and analysis of the current most popular DDoS attack types and mitigations.

In this survey, we have presented a complete analysis on the generation and mitigation of the current largest DNS reflection attack with more than 300 Gbps on Spamhaus.org. This analysis is followed by a discussion on the current most popular DDoS attack types (DNS Reflection Attacks, SYN floods, UDP floods, ICMP floods and HTTP Flood Attacks) in the Infrastructure and Application layers.

For combating the current most popular DDoS attack types presented in this survey, we have extensively discussed various effective cloud-based DDoS mitigation and protection techniques that have been proposed by both the academic researchers and large commercial cloud-based DDoS service providers.

REFERENCES

[1] M. Prince, "The Ddos That Knocked Spamhaus Offline (And How We Mitigated It)," Vol. 2013, Ed: Cloudflare, March 20, 2013 P. Web Log Post.

[2] Prolexic Technologies, "Prolexic Quarterly Global Ddos Attack Report Q1 2013," Florida2013.

[3] Akamai Technologies. (2013). The State Of The Internet 4th Quarter, 2012 Report. 5. Available: Http://Www.Akamai.Com/Dl/Akamai/Akamai_Soti_Q412_Exec_Summary.Pdf

[4] D. Anstee, D. Bussiere, And G. Sockrider. (2013). Worldwide Infrastructure Security Report 2012 Viii. Available: Http://Pages.Arbornetworks.Com/Rs/Arbor/Images/Wisr2012_En.Pdf

[5] Cert. (2013, April 15). Dns Amplification Attacks And Open Dns Resolvers. Available: Https://Www.Cert.Be/Pro/Docs/Dns-Amplification-Attacks-And-Open-Dns-Resolvers

[6] G. Lindsay. (2012, March 10). Dnssec And Dns Amplification Attacks. Available: Http://Technet.Microsoft.Com/En-Us/Security/Hh972393.Aspx

[7] R. Beverly And S. Bauer, "The Spoofer Project: Inferring The Extent Of Source Address Filtering On The Internet," Presented At The Proceedings Of The Steps To Reducing Unwanted Traffic On The Internet On Steps To Reducing Unwanted Traffic On The Internet Workshop, Cambridge, Ma, 2005.

[8] P. Vixie. (August 1999, Rfc 2671 , Extension Mechanisms For Dns (Edns0). Available: Http://Tools.Ietf.Org/Html/Rfc2671

[9] Dnssec.Net. (2013). Dnssec: Dns Security Extensions Securing The Domain Name System. Available: Http://Www.Dnssec.Net/

[10] T. Peng, C. Leckie, And K. Ramamohanarao, "Survey Of Network-Based Defense Mechanisms Countering The Dos And Ddos Problems," Acm Comput. Surv., Vol. 39, P. 3, 2007.

[11] W. M. Eddy, "Defenses Against Tcp Syn Flooding Attacks," The Internet Protocol Journal Vol. 9, 2006.

[12] D. S. Paul Ferguson. (2000, Network Ingress Filtering: Defeating Denial Of Service Attacks Which Employ Ip Source Address Spoofing. 1-10. Available: Http://Www.Ietf.Org/Rfc/Rfc2827.Txt

[13] Cert. (1997, Cert® Advisory Ca-1996-01 Udp Port Denial-Of-Service Attack. Available: Http://Www.Cert.Org/Advisories/Ca-1996-01.Html

[14] T. Bowman, "Incident Handling And Hacker Exploits Certification Practical Version 1.5c," Sans Institutemay 10, 2013 2001.

[15] M. Sauter, ""Loic Will Tear Us Apart": The Impact Of Tool Design And Media Portrayals In The Success Of Activist Ddos Attacks," American Behavioral Scientist, P. 0002764213479370.

[16] M. Prince, "Deep Inside A Dns Amplification Ddos Attack," Vol. 2013, Ed: Cloudflare, October 30, 2012 P. Web Log Post.

[17] Cert. (2000, Cert® Advisory Ca-1998-01 Smurf Ip Denial-Of-Service Attacks. Available: Http://Www.Cert.Org/Advisories/Ca-1998-01.Html
[18] C. A. Huegen. (2000, The Latest In Denial Of Service Attacks: "Smurfing" Description And Information To Minimize Effects. Available: Http://Www.Pentics.Net/Denial-Of-Service/White-Papers/Smurf.Cgi
[19] A. Litan. (2013, Arming Financial And E-Commerce Services Against Top 2013 Cyberthreats. Available: Http://Www.Gartner.Com/Technology/Reprints.Do?Id=1-1f9xfpx&Ct=130429&St=Sb
[20] S. Mcgregory, "Preparing For The Next Ddos Attack," Network Security, Vol. 2013, Pp. 5-6, 5// 2013.
[21] Arbor Networks, "The Growing Threat Of Application-Layer Ddos Attacks," 2012.
[22] S. Ranjan, R. Swaminathan, M. Uysal, And E. Knightly, "Ddos-Resilient Scheduling To Counter Application Layer Attacks Under Imperfect Detection," In Infocom 2006. 25th Ieee International Conference On Computer Communications. Proceedings, 2006, Pp. 1-13.
[23] D. Watson, "Web Application Attacks," Network Security, Vol. 2007, Pp. 10-14, 10// 2007.
[24] C. Linhart, A. Klein, R. Heled, And S. Orrin, "Http Request Smuggling," Computer Security Journal, Vol. 22, Pp. 13-26, 2006.
[25] S. Heron, "Denial Of Service: Motivations And Trends," Network Security, Vol. 2010, Pp. 10-12, 5// 2010.
[26] T. Rozekrans And J. D. Koning. (2013, Defending Against Dns Reflection Amplication Attacks. System & Network Engineering Rp1.
[27] S. Lima, "3 Ways To Use Dns Rate Limit Against Ddos Attacks," Vol. 2013, Ed: Cloudshield January 29, 2013 P. Web Log Post.
[28] I. Avramopoulos And M. Suchara, "Protecting The Dns From Routing Attacks: Two Alternative Anycast Implementations," Security & Privacy, Ieee, Vol. 7, Pp. 14-20, 2009.
[29] Cert. (2012, May 7). "Anonymous" Ddos Activity. Available: Http://Www.Us-Cert.Gov/Ncas/Alerts/Ta12-024a
[30] A. S. Aiko Pras, Giovane C. M. Moura, Idilio Drago, Rafael Barbosa, Ramin Sadre, Ricardo Schmidt, Rick Hofstede, "Attacks By “Anonymous” Wikileaks Proponents Not Anonymous," University Of Twente, Enschede, The Netherlands2010.
[31] T. Komatsu And A. Namatame, "On The Effectiveness Of Rate-Limiting Methods To Mitigate Distributed Dos (Ddos) Attacks(<Special Section>New Challenge For Internet Technology And Its Architecture)," Ieice Transactions On Communications, Vol. 90, Pp. 2665-2672, 2007/10/01 2007.
[32] G. Muharremoğlu. (2012) Web Application Level Approach Against The Http Flood Attacks : Iosec Http Anti Flood/Dos Security Gateway Module. Hakin9 - It Security Magazine. 56-59. Available: Http://Www.Iosec.Org/Hakin9_11_2012_Iosec.Pdf
[33] P. Chwalinski, R. Belavkin, And X. Cheng, "Detection Of Http-Get Attack With Clustering And Information Theoretic Measurements," In Foundations And Practice Of Security. Vol. 7743, J. Garcia-Alfaro, F. Cuppens, N. Cuppens-Boulahia, A. Miri, And N. Tawbi, Eds., Ed: Springer Berlin Heidelberg, 2013, Pp. 45-61.
[34] D. Das, U. Sharma, And D. K. Bhattacharyya, "Detection Of Http Flooding Attacks In Multiple Scenarios," Presented At The Proceedings Of The 2011 International Conference On Communication, Computing & Security, Rourkela, Odisha, India, 2011.

Authors

Fui Fui Wong is currently a Ph.D. candidate in the Department of Computer Science and Technology, at TongJi University, China. She received her Master of Information and Communication Technology from University of Wollongong, Australia in 2004. Her research interests are Network Security and Cloud Computing.

Prof. Dr. Cheng Xiang Tan is a Professor at the Department of Computer Science and Technology of TongJi University, China. He received his Ph.D. degree from Northwestern polytechnical university, China in 1994. He is a member of the Information Security Standardization Commission, China Ministry of Public Security, Consultant for China State Project Anti-Cybercrime Computer Forensics, and founding Vice President of China State Research Centre Against Computer Attacks and Virus. His research activity is focus on information security, cell phone and mobile security with a special interest in digital forensics.