International Journal for Modern Trends in Science and Technology
Volume: 03, Special Issue No: 01, February 2017
ISSN: 2455-3778
http://www.ijmtst.com

DDoS Attacks, Detection Parameters and Mitigation in Cloud Environment

K.Santhi Sri[1] | PRSM Lakshmi[2]

[1]Associate Professor, Department of CSE, Vignan's University, Guntur, A.P, India.
[2]Assistant Professor, Department of CSE, Vignan's University, Guntur, A.P, India.

To Cite this Article
K.Santhi Sri and PRSM Lakshmi, "DDoS Attacks, Detection Parameters and Mitigation in Cloud Environment", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Special Issue 01, 2017, pp. 79-82.

ABSTRACT

Cloud computing refers to providing on demand services and computing resources via Internet. The cloud environment has many security challenges among which DDoS attcks have maximum priority. Within Cloud Security issues being dominant for the private enterprises, the denial of service attacks are rated as the highest priority threat. This paper presents a review of DDoS attacks and parameters to detect attacks and mitigation mechanisms.

KEYWORDS: *Cloud Computing, Cloud Security, DoS, DDoS, Distributed Denial of Service*

I. INTRODUCTION

In order to determine the DDoS attack, existing academic literature research work from 2009 to 2015 is surveyed from IEEE, ACM Science Direct, Elsevier and ACM, searching for keywords as Cloud Security, DDoS Mitigation, Detecting DDoS, Hybrid Cloud, Network Architecture, Packet Flooding, SYN Flood, TCP Flood, UDP Flood. The papers are classified in terms of Infrastructure level Direct Network layer attacks, For Infrastructure level Direct Application layer attacks. New Taxonomy for classifying DDoS Attacks is also proposed in the paper by Degree of Attack Automation, Exploitation of Vulnerabilities, Attack Rate Dynamics and Impact of DDoS Attacks. This section reviews related research work that has already been carried out in the same domain area. The author surveyed several research publications from IEEE, ACM, Science Direct and other digital libraries between 2009 and June 2016 using keywords as mentioned below and in the Figure 1 for DDoS attacks like Cloud Security, DDoS Mitigation, Detecting DDoS, Hybrid Cloud, Network Architecture, Packet Flooding, SYN Flood, TCP Flood and UDP Flood.With the advances in technology, new powerful attack tools available for launching DDoS attacks, the attack trends and threats security offered is not static. This trend forces the cloud service providers to maintain state-of-art defenses in order to stay ahead of the most recent attack. The main focus of a network security attack is to be able to infiltrate, crash data center devices or alter configuration information, adversely impacting the uptime, availability, reputation, productivity, quality of service and the revenue of the service providers.

While a number of research surveys have been published on the DDoS topic, this survey is different from them in the following manner:

In Wong and Tan (2014) focused on DDoS attacks on Cloud infrastructure [1] and application systems, while DDoS attack and DDoS Mitigation are the focus for this survey. Several other surveys and conference papers are of limited scope, in Darwish et al. (2013) [2]. Consequences of DDoS attacks against a cloud environment were

highlighted in some review papers as well by Anwar and Malik 2014 for DDoS attacks [3] on cellular network were explained by Merlo et al (2014), while Hybrid cloud environment architecture design is focused here.

The below section presents a classification as Figure 2 for the DDoS attacks as per degrees of automation,vulnerabilities exploited, attack rate dynamics and impact of the attack.

1. As per Degree of Attack Automation

The Manual attacks involve the attacker scanning the network, IP Addresses, machines for vulnerabilities, break into the system and deploy a code and executes a malicious payload for remote control access of that user system which is kept ready to launch an attack on the attackers command. Semi-automatic attacks involve deploying attack scripts that scan and compromise the user machines and download a payload and installing the attack codes. These victim systems are bots under control of the handlers who choose when and how about the attack type and target victims. Automatic attacks on the other hand are carried with a high degree of automation, with the compromised user systems having the attack code and software with predetermined type of attack, duration, victim's IP address. The attacker has minimal interaction once the payload gets deployed or during the automatic attack.

2.As per Exploitation of Vulnerabilities

Bandwidth Depletion attacks involve flooding and amplification clogging the WAN pipes with attack network packets. Flooding involves bots and zombies sending huge volumes of traffic to clog and congest the target's bandwidth pipes. The response from the victim slows down with the increase in such flood requests, saturating the bandwidth pipe, preventing access to the authorized users. Amplification attacks involve the bots and zombies sending messages to the target's subnet by broadcast. Resource Depletion attacks involve use of malformed data packets having incorrect IP packets being sent by the zombies with the malicious intent to crash it and protocol exploits which involve exploitation of a specific protocol feature to have the victim consume resources and ultimately make it unavailable to the legitimate users.

3. As per Attack Rate Dynamics

Continuous and variable rate DDoS attacks are most common. Continuous rate attacks are executed without break or lowering the force of attack. This leads to the disruptions in services quickly however, this attack gets detected as well. Variable rate attacks vary the attack frequency and force, carefully avoiding detection which ranges from having the attack increase in force or have a fluctuating rate of attack.

4.As per the Impact of Attacks

Disruptive and degrading are two common types of attack. While the impact of disruptive attacks is complete shutdown and leads to full denial of services to the legitimate clients. Recovery from such disruptive attacks has the impact based on automated self-healing recovery, Human intervention and non-recoverable. Degrading attacks consume the victim resource bit by bit in small portions. This is much smarter than other attacks, making the attack difficult to detect.

For Infrastructure level Direct Network layer attacks: For TCP Flood attacks where Transmission Control Protocol (TCP) having a three way handshake prior to establishing actual packet exchanges with connection orientated protocol features. Each SYN message sent by a connecting host is acknowledged with SYN + ACK and the handshaking process completes with ACK, finally establishing a connection between two hosts. Attackers exploited this three way handshake feature by initiating connections which were half-open, leading to huge number of transmission block allocations exhausting the kernel memory (Wong and Tan 2014). Zargar et al. (2013) researched on network and transport layer protocols to flood a host using TCP SYN, UDP and ICMP floods. Exploiting TCP SYN for half open connection feature leading to large number of transmission block allocations causing exhaustion of kernel memory was examined by Wong and Tan (2014). Amazon Cloud Services being affected by TCP SYN floods were reported by Cha and Kim (2011).

For Infrastructure level Direct Application layer attacks: HTTP Flood Attacks on Application layer target cloud services by sending web packet floods at high rates to overwhelm a target web application server using malformed HTTP packets (Choi et al. 2014). These consume the target cloud web server's resources preventing legitimate users from accessing the services as also such attacks are challenging to mitigate since these consume very little bandwidth flow and are mostly stealthy. The target server gets inundated with HTTP and SML floods which appear as legitimate GET and POST requests (Wong and Tan, 2014). Wong and Tan (2014) reported that one fourth of the global DDoS attacks target the application layer while HTTP GET floods comprise of one fifth of the global

HTTP attacks. Mina Tahmasbi, Albert Greenberg, Dave Maltz, Jennifer Rexford and Lihua Yuan (2012) [38] present a scalable network-application profiler (SNAP) that guides the engineers to identify and fix performance related issues. This passively ensures the TCP statistics are collected, logs from socket-call having low overhead for computation and storage across shared computing resources like servers, circuits or switches and connections to pinpoint the location of the problem like TCP/application conflicts, application-generated micro-bursts, network congestion or sending buffer mismanagement. SNAP combines socket-call logs of data-transfer behaviors with TCP for the application from the network stack that highlight the data delivery. The profiler leverages the topology, network routing, and application deployment in the data center to correlate performance issues for network connections and aims to find the congested resource or problematic software component. The SNAP deployment is done in a real time production data center running over 8,000 servers and over 700 application components that uncovered over 15 major performance issue in the web application software, the network stack on the server, and the underlying network.

II. PARAMETERS FOR AN EFFECTIVE DDOS DETECTION SOLUTION

After reviewing the above mentioned research manuscripts for DDoS attack issues and classification attacks, the following parameters are selected for determining an effective DDoS detection method.

Real time Response Detection mechanism – those methods with real time, high speed, immediate or proactive response mechanisms for Advanced Application Attacks and Cloud Diversion attacks that have the ability to reduce the attack surface for say routing inbound Accuracy of Defense Mechanism – is a critical parameter to judge the detection mechanism regards to Sensitivity (True Positive or True Negative ratio), Reliability (False Positive or False Negative ratio) for the desired outcomes.

Over-Under Mitigate – detection effectiveness is also measured on the vendor's ability to mitigate as per Rate-Only, HTTP Server based Redirects, SSL Protections, Routing Techniques, Heuristic Behavior, JavaScript Challenge Response and Signature

Reporting – determine how well and traffic or have network ACLs that create stateless allow-and-deny rules in case of attacks are definitely effective as compared to reactive detection mechanisms

Ability to auto scale – dynamic, auto scalability mechanisms that can handle flood attack, scale up bandwidth links or even utilize elastic load balancing (ELB) to have better fault tolerance in case of increase in attackers

Throughput – end to end time taken for the request generated by a legitimate clients for the server. The ability to sustain high levels of throughput determines the DDoS effectiveness.

Request Response Time – relates to the average time for a successful HTTP response. With the increase in attack rate, processing capability impacts the request response.

Zero Day Attack Detection Ability – being able to detect new, unknown attacks covering OWASP vulnerabilities as well as ranging from Netflow, Headerless Layer7 packet, Open Flow, OOP Synchronous, Software Defined Networking (SDN) to feeds from Partners/Works with Other Vendor Signals.

Performance Degradation – due to resource crunch of CPU cycles, Memory, Storage or network bandwidth effective is the detection reported. Parameters taken into account are Real-Time Displays, All Attacking Vectors Granularly, Attack-Back Options, Mitigation Response, Mitigation Response – Real Time, Historical Mitigation Effectiveness Measure, Forensics Reports, Legitimate and attack Traffic Displayed, Emergency Response Options and Mitigation Response and Integrated Reporting with Cloud Portals.

III. PROPOSED PARAMETERS FOR DDOS COUNTERMEASURE

While a number of research proposals and partial DDoS mitigation solutions are available as discussed above, most of these only assist in preventing very few aspects of the full DDoS attack. There seems to be no one shot comprehensive countermeasure against each known DoS attack. Every day, attackers keep coming up with new vector threats and attack derivatives in their attempts to bypass existing and new countermeasures deployed. This leads us to the conclusion the more research is required when trying to design and develop an effective DDoS countermeasure solution.

The ideal time to mitigate a DDoS attack is right at the launching location and stage by not allowing it to reach the target or even travel over WAN circuits.

However, achieving this is far from implementation.

Classification, analysis and comparison of DDoS tools is performed by the research authors for a better understanding of the existing tools, methods and attack mechanism along with a study of DDoS tools. This will provide a better understanding of DDoS tools in present times. DDoS research papers since January 2009 to March 2016 are categorized in the preceding section as per application level and infrastructure level attacks. From the literature survey performed, most of the research papers are directed towards Infrastructure level DDoS attacks primarily due to the ease with which the Infrastructure attacks for network and application floods can be performed.

In Infrastructure level attacks, there is no exploitation of vulnerability, the attackers flood the bandwidth pipes with malicious traffic and consume computing resources, denying legitimate access to authenticated users.

Application attacks on the other hand, exploit system and web application vulnerabilities at OSI layer 7 mimicking human behavior related to system weakness, outdated patches and misconfigurations while carrying out the attack.

IV. Conclusion

This paper provides a survey of the academic literature on DDoS attacks against cloud computing from 2009 to 2015. New cloud attack taxonomy and parameters to determine effective DDoS solution is presented. A comprehensive DDoS mitigation solution involves detection, blocking and mitigation in real time as well as be positioned at the DDoS attack source. For this the DDoS detection nodes need to be spread across the internet globally. These nodes are used for the DDoS attack detection, response and prevention. Apart from this feature, the following factors need to be considered for the proposed DDoS mitigation solution as

REFERENCES

[1] Wong F, Tan C X, "A Survey of Trends in Massive DDoS Attacks and Cloud-based Mitigations", International Journal of Networks Security Applications (IJNSA), 2014, vol. 6(3), pp 57–71.

[2] Darwish M, Ouda A, Capretz L F, "Cloud based DDoS Attacks and Defenses", IEEE International Conference on Information Society, 2013, pp 67–71.

[3] Anwar Z, Malik A, "Can a DDoS Attack melt down my data center? A Simulation Study and Defense Strategies", IEEE, 2014, vol. 18(7), pp 1175–8.

[4] Zargar S T, Joshi J, David T, "A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE Communication Survey Tutor, 2013, vol. 15(4), pp 2046–69.

[5] Idziorek J, Tannian M, Jacobson D, "Attribution of Fraudulent Resource Consumption in the Cloud", 5th IEEE International Conference on Cloud Computing (CLOUD), 2012, pp 99–106.

[6] Ficco M, Palmieri F, "Introducing Fraudulent Energy Consumption in Cloud Infrastructures: a new generation of Denial-of-Service Attacks", IEEE System Journal, 2015 vol. 99, pp 1–11.

[7] Chonka A, Abawajy J, "Detecting and Mitigating HX-DoS attacks against Cloud Web Services", 15th IEEE International Conference on Network based Information Systems (NBiS), 2012, pp 429–34.

[8] Rui X, Wen-Li M, Wen-Ling Z, "Defending against UDP Flooding by Negative Selection Algorithm based on EIGEN value sets", 5th IEEE International Conference on Information Assurance and Security (IAS'09), Xi'an, China, 2009, vol. 2, pp 342–5.

[9] Bhuyan M H, Bhattacharyya D K, Kalita J K, "An Empirical Evaluation of Information Metrics for low rate and high rate DDoS Attack Detection", Pattern Recognition Letter, 2015, vol. 51, pp 1–7.

[10] Choi J, Choi C, Ko B, Choi D, Kim, P P, "Detecting web based DDoS attack using Map Reduce operations in cloud computing environment", Journal of Internet Security and Information Security", 2013, vol. 3(3–4), pp 28–37.

[11] Karnwal T, Sivakumar T, Aghila G, "A Comber approach to protect Cloud Computing against XML DDoS and HTTP DDoS attacks", IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, 2012, pp 1–5.

[12] Gruschka N, Iacono L L, "Vulnerable Cloud: Soap Message Security Validation Revisited", IEEE International Conference on Web Services (ICWS 2009), Los Angeles, 2009, pp 625–31.

[13] Arukonda S, Sinha S, "The Innocent Perpetrators: Reflectors & Reflection Attacks", Advances in Computer Science International Journal, 2015, pp 94–8.

[14] Lonea A M, Popescu D E, Prostean Q, Tianfield H, "Soft Computing Applications Evaluation of Experiments on Detecting DDoS attacks in Eucalyptus Private Cloud", 2013, pp 367–79.

[15] Bakshi A, Yogesh B, "Securing Cloud from DDoS attacks using Intrusion Detection system in virtual machines", 2nd IEEE International Conference on Communication Software and Networks (ICCSN'10), Singapore, 2010, pp 260–4.

[16] Kwon H, Kim T, Yu SJ, Sim HK, "Self-similarity based light weight Intrusion Detection method for Cloud Computing", 3rd International Conference on Intelligent Information and Database systems (ACIIDS), Daegu, Korea, 2011, pp 353–62.

[17] Modi C, Patel D, Borisaniya B, Patel H, Patel A, Rajarajan M, "A Survey of Intrusion Detection Techniques in Cloud", Journal of Network and Computer Applications, 2013, vol. 36(1), pp 42–57.