International Journal of Computing and Applications | **ISSN: 0973-5704**
Volume 13, Number 1, (January-June 2018), pp 23-28

A REVIEW OF DDOS ATTACKS IN CLOUD ENVIRONMENT

Pankaj Sharma[1] and Ankur Gupta[2]

[1-2]Model Institute of Engineering and Technology, Jammu, India.
Email: [1]pankaj.cse@mietjammu.in, [2]ankurgupta@mietjammu.in

Abstract: DDoS attacks have gained notoriety in the recent past due to their propensity for causing large scale disruption across cloud service providers. The prevalence of DDoS attacks on cloud infrastructure resulting in the potential inaccessibility of data and severe impact on quality-of-service is a deterrent for potential customers in adopting the cloud business model. This research paper reviews the impact of DDoS attacks on cloud infrastructure, and finally compares and contrasts the various mechanisms available for dealing with DDoS attacks. It finally presents the open challenges and lists some future strategies to potentially counter the menace of DDoS attacks.

Keywords: DDoS; Defense; detectection; Prevention.

1. INTRODUCTION

In the preceding years, DDoS attacks [1] have become more common due to their easy instigation and damage to their proposed targets. The complex architectural structures of DDoS attacks make the source of the attacks even difficult to mitigate and trace. According to John N. Stewart senior vice president and chief security officer at Cisco, "DDoS attacks must be a peak security consideration for organizations in the private and public sector in 2014" [2]. China, USA and Canada were the countries that faced the largest number of DDoS attacks and China was on the top of the list of source of attacking IPs [3]. The largest DDoS attack in history was 600 Gbps DDoS attack on BBC occur in January 2016 [4]. One of the reasons why DDoS attacks focus on these countries is because they have the most important Internet Data Centers (IDCs) carrying popular Internet services [5][6][7] [9][10].As per economic impact of DDoS attack 9% of organizations in the world would lose $500,000-$1 million or more per hour in a peak-time DDoS related attacks. 10% would lose approximately $250K or more [13]. DDoS attacks classified into two key categories. One based on the computational resource exhaustion and another based on the bandwidth exhaustion. Resource exhaustion attacks mortify the capacity of the device to function, such as opening many concurrent connections to a particular device. Bandwidth exhaustion attempt to overwhelm the bandwidth capacity of the network [11]. DDoS attacks are typically launched in the forms of SYN flood, UDP flood and TCP- SYN flooding, these attacks are instigated by crafting packets from spoofed address and generating a high number of half-open connections[12]. Prolexic reported that the majority of attacks were TCP (SYN, PUSH, ACK), UDP and HTTP[10]. One of the key reason that make the DDoS attacks wide spread and easy on the Internet is the accessibility of attacking tools and the power of these tools to generate aggressive traffic. There are different DDoS attack tools on the Internet that allow attackers to perform attacks on the target system[13].

2. DDOS DEFENSE MECHANISMS

Several DDoS detection and prevention mechanism already exist, but the fool-proof DDoS defense remains elusive. There are several key technical challenges which make the task of designing the perfect DDOS defense daunting [11]. But generally, the moment DDOS attack is detected, nothing else can be done apart

from disconnecting the victim from resources. After the victim is detached, the attack source identification and trace back can be carried out. As shown in figure 1 [6] companies are still fighting with DDoS attacks and no any specific tools are designed for combating with DDoS attack. Approximately two-thirds of companies use conventional solutions like traditional firewalls, routers, switches and intrusion prevention systems (IPS) to defend against DDoS attacks[12] [31].

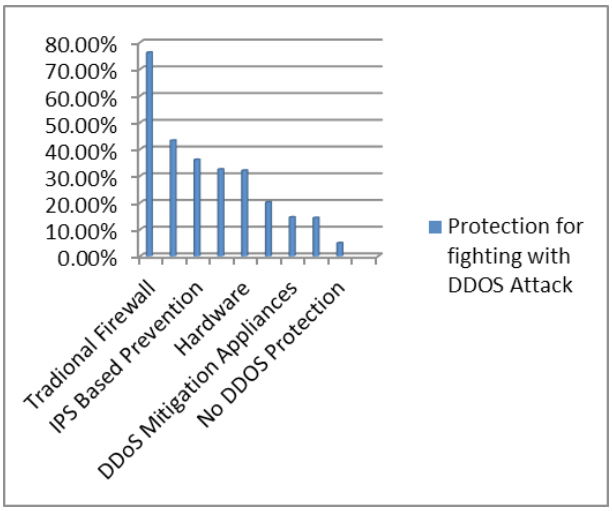

Figure 1: Protection techniques against DDOS Attacks[6] [31].

More companies are embracing purpose-built DDoS solutions but not succeeding. Companies with no DDoS protection dropped from 8 percent to less than 5 percent[6][31]. DDoS attacks are growing in complex, dangerous ways. Almost 90 percent of those attacked were hit frequently. Table I depict the features and shortcomings of different DDoS defense mechanisms. There is also a significant difference between these mechanisms either due to the location, protocol or way of defending. As shown in fig 1, DDoS detection is the core requirement of the DDoS defense process. Prevent forged packets from reaching the destinations while allowing authentic packets to pass through and dropping all packets forwarded to the victim when a threat is detected is another challenge. Mitigation from DDoS avoidance and recovery is not very easy, so that's why we take avoidance and recovery at higher level of complexity.

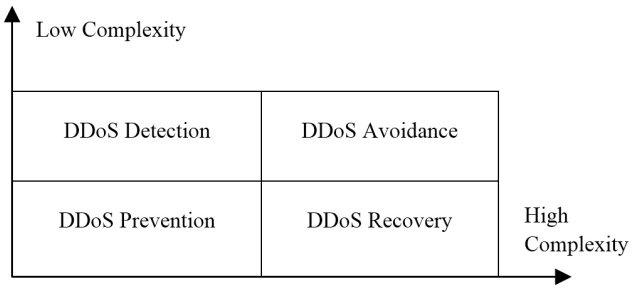

Figure 2: The DDoS Mitigation Quadrant.

3. CHALLENGES IN DEVISING DDOS DEFENSE MECHANISMS

The defense mechanisms reviewed in this paper are far from adequate to protect Internet nodes from DDoS attacks. The main problem is that there are still many insecure areas on the Internet that can be compromised to launch large-scale DDoS attacks. The key challenges in detection and prevention of DDoS attack are:

A. Diversity and Scale of Sources

Sources are disseminated among various domains, it is difficult for each of the node to detect and filter legitimate traffic accurately comes from the different sources. DDoS attack mitigations at the single source might be simple than multiple sources [30].

B. High Network Traffic and Computations

DDoS is an organized attack technique with a group of distributed infected devices across the Internet with the purpose of simultaneously sending a large volume of forged or look like genuine packets to a particular victim. As per the classification of DDoS attack mainly consume the network bandwidth and exhaust the computational resources by sending large amount of packets over the internet[25].

C. Difficulty in Differentiating the Malicious Packet from Legitimate Traffic

Many approaches are proposed [18], for differentiating the malicious packet from legitimate traffic, but all technique based on the analysis of past traffic patterns, malicious packet can adopt the behavior of genuine traffic and under some circumstances or due to non uniqueness of DDoS packet stream legitimate packets

Table 1
Summary of DDOS detection and prevention technique

S. No.	*Methods*	*Deployment Classification*	*Privacy Preserving*	*Feature*	*Limitation*
1.	Intrusion Detection System [6][17].	Time of action Based	No	This technique secure cloud environment from single point of failure.	1. This method scrutinize for Particular malicious packet. 2. Not designed to handle high-volume DDOS attacks
2.	Intrusion prevention system [25][27].	Time of action Based	No	Intrusion Prevention System can work as an anomaly detector	IPS devices are restricted to the number of TCP sessions and amount of bandwidth utilization at a given moment
3.	Confidence Based Filtering Approach[16].	Protocol Based	No	Small storage size for nominal profile and high packet filtering efficiency	Confidence based filtering approach Does not have high accuracy than Other technique
4.	Firewalls [6].	Time of action Based	No	Firewall was the first choke point devices used to separate trusted from non trusted network.	1. Proxy servers required for the implementation of firewalls that can intensify DDoS attacks by expanding the attack surface 2. Firewall may reduce the memory of the firewalled device
5.	Cloud trace back model [25].	Location Based	No	1. Averts direct DDoS with CTB 2. Identity of attacker will be made known during successful DDoS attack	Computational overhead increases for overall performance
6.	A filter tree approach to defend against XML/HTTP DDoS Attack[30].	Protocol Based	No	1. Filter attacks in several stages. 2. The client request is converted to XML format and then the SOAP message is embedded and signed with client IP address	This approach Can detect only application layer DDOS Attack and fails to detect DDoS attacks in transport and network layers
7.	Virtualization strategy to secure cloud environment from DDoS attack[24].	Location Based	No	1. It analyze incoming and outgoing packet. 2. Applications are shifted to other virtual machine at different data centre on the detection of DDOS attack and packets from malicious node are blocked	This technique prohibited only known attacks, hence all type of DDOS attack are not detected in virtualized environment
8.	Neural classifier for detecting DDoS Attack [26].	Location Based	No	This method provides high detection accuracy with less false positive results.	1. Collecting proper training data set for neural network is difficult 2. Performance depends on accuracy of training data set

can act like non legitimate packets. Due to lack of improper attack information and inefficient evaluation technique, DDoS attacks is not properly defensive [13][25]. Appropriate testing approaches should be engage to detect either a particular node or intermediate network endures a DDoS attack or not .Sometimes during peak hours resources are not available, and we think that it's a attack period.

D. Privacy Violations

DDoS defense mechanism like Firewalls, IDS and filtering approaches violates the privacy of the authentic user, because all incoming and outgoing packets need to be inspected. Privacy anxiety always take place whenever sensitive data is outsourced to the network or cloud.

E. Masked Character of Attackers and Vulnerabilities in the Internet

Attackers usually make use of spoofed IP addresses in order to conceal their true identity, which makes DDoS mitigations more difficult. It is very difficult for the defense mechanisms to identify the original attacker because of the use of spoofed IP addresses [31]. Almost all resource that is connected to the Internet is vulnerable to DDoS attacks, many existing controls do not protect against these attacks. Attackers will use a massive range of vulnerable hosts to initiate an attack rather than employing a single server. These Vulnerabilities might be the weaknesses in the network or security policy [23]. The attackers exploit these weaknesses by inserting malicious code or other hacking tools and technique so that they become under his control. These defenseless can be in hundreds or thousands in numbers.

F. Lack of Organizational Domain Collaboration

Different organizations all over the world work independently to deals with DDoS, but there is a need to understand that if these organizations work together then they can create a better defensive technique against these attacks. Organizations may make alliance in the field of research and development for DDoS mitigations.

4. CONCLUSIONS & FUTURE SCOPE

This paper presents an overview of the DDoS attack and the commonly employed defense strategies. It is clear that DDoS associated downtime represents a vital threat to any organization that relies on IT assets to carry out its business. An efficient DDoS mitigation solution can help organizations handle risk by avoiding financial risks and service downtime associated with a DDoS attack. The current prevention mechanisms reviewed in this paper are effective yet far from optimal in providing complete security for DDoS attack. The key difficulty is that there are still many machines over the Internet that can be compromised to launch DDoS attack. Some future directions in this critical domain are:

- Group several stages of defense activities to trap variety of DDoS attack. If one stage of defense mechanism fails, then the others still have the possibility to defend against attack. Multi-tier detection and prevention policies need to be applied on multiple locations.
- Proactive mechanisms are mandatory to authenticate the sources of the traffic so that malicious nodes could be identified.
- Novel high-availability solutions may have to be adopted to ensure business continuity.
- Preserving privacy is another significant concern with regards to DDoS attack in cloud computing, existing DDoS detection and prevention rely on traffic analysis is putting customer confidentiality at risk.
- A coordinated strategy across CSPs would ensure that cloud infrastructure cannot be used to launch DDoS attacks. Using inexpensive cloud resources to launch DDoS attacks has empowered almost any malicious users to launch global attacks. Some early work done in this direction can be found in [28].

References

[1] P.J. Criscuolo, Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory

Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.

[2] Cisco annual security report 2014. www.cisco.com/web/offer /gist_ty2_asset/Cisco_2014_ASR.pdf.

[3] Akamai's report Q1 2016. www.akamai.com. /…/ stateoftheinternet

[4] http://betanews.com/2016/01/12/bbc-was-hit-with-the-biggest-ever- ddos-attack/

[5] US State of Cybercrime Survey report 2014.http://www.pwc.com/us/en/increasing-it-effectiveness / publications/assets/2014-us-state-of-cybercrime.pdf.

[6] Neustar Annual DDoS Attacks and Impact Report "the danger deepens" 2014. https://www.neustar.biz/resources/whitepapers /ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf.

[7] DDOS and downtime considerations for risk management, verisign white paper. www.verisigninc.com/assets/whitepaper-ddos-risk-management.pdf.

[8] Statistics on botnet assisted DDoS attacks in Q1 2015. http://www.slideshare.net/KasperskyLabGlobal / statistics-on-botnet- assisted-ddos-attacks-in-q1-2015.

[9] Huawei Cloud Security Center survey report on Botnets and DDoSAttacks 2013. enterprise.huawei.com /ilink.enenterprise/download/HW_315881.

[10] Prolexic quarterly global ddos attack report Q2 2014. http://www.prolexic.com/kcresources/attack-report/ attack_report_q214/Prolexic-Q22014-Global-Attack-Report-A4.pdf.

[11] Neustar Annual DDoS Attack and Impact Survey 2012. https://www.neustar.biz/enterprise/.../ddos.../2012- ddos-attacks-report.pdf.

[12] Cisco ddos protection solution delivering "clean pipes" Capabilities for service providers and their customers white paper.

[13] Christos Douligeris, Aikaterini Mitrokotsa "DDoS attacks and defense mechanisms: classification and state-of the-art " Elsevier Computer Networks 44 (2004) pp 643–666.

[14] J. Idziorek, M. Tannian, and D. Jacobson, "Attribution of Fraudulent Resource Consumption in the Cloud," Proc. 2012 IEEE 5th Int'l Conf. Cloud.Computing (Cloud 12), IEEE, 2012, pp. 99–106.

[15] Stephen M. Specht and Ruby B. Lee, Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. 17th International Conference on Parallel and Distributed Computing Systems, 2004, pp. 543-550.

[16] Chen, Qi, W. Lin, W. Dou, Shui Yu. "CBF: A packet filtering method for DDoS attack defense in cloud environment," IEEE Ninth International Conference on Dependable Autonomic and Secure Computing,, Sydney, 2011, pp. 427-434.

[17] K.Vieira, A. Schulter, Carlos Westphall, Carla Westphall, "Intrusion detection for grid and cloud computing." It Professional, Vol. 12, No. 4, pp. 38-43, July 2010.

[18] Basheer Al-Duwairi, Manimaran Govindarasu, "Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback", IEEE transaction on parallel and distributed system, Vol. 17, No. 5, May 06.

[19] L.C. Chen, T.A. Longstaff, K.M. Carley, "Characterization of defense mechanisms against distributed. denial of service attacks", Computers & Security, Vol. 23, No. 8, December 2004, pp. 665-678.

[20] T. Peng, C. Leckie, and K. Ramamohanarao," Survey of network-based defense mechanisms countering the DoS and DDoS problems", ACM Computing. Survey. 39, 1, Article 3, April 2007.

[21] L. Garber, "Denial-of-service attacks rip the Internet," IEEE Computer, Volume 33, Issue 4, pp. 12–17, Apr. 2000.

[22] R.K.C. Chang, Defending against flooding-based distributed denial of service attacks: A tutorial, Computer journal of IEEE Communications Magazine, Vol. 40, No. 10, 2002, pp. 42-51.

[23] K. Lee, J. Kim, K.H. Kwon, Y. Han, and S. Kim, "DDoS Attack Detection Method Using Cluster Analysis," Expert Systems with Applications, Vol. 34, No. 3, 2008, pp. 1659-1665.

[24] Ryan Shea, Student Member, IEEE, and Jiangchuan Liu, Senior Member, IEEE "performance of virtual machines under networked denial of service attacks: experiments and analysis" ieee systems journal, Vol. 7, No. 2, june 2013, pp. 335-345.

[25] Saman Taghavi Zargar, Member IEEE, James Joshi, Member, IEEE, and David Tipper, Senior Member, IEEE "A Survey of Defense Mechanisms Against

Distributed Denial of Service (DDoS) flooding attacks" ieee communications surveys & tutorials, Vol. 15, No. 4, fourth quarter 2013, pp. 2046-2069.

[26] R. Kumar, P. Arun, S. Selvakumar, "Distributed denial of service attack detection using an ensemble of neural classifier," International Journal of Computer Communications, Vol. 34, No. 11, 2011 pp. 1328-1341.

[27] B. B. Gupta, R. C. Joshi, and Manoj Misra, Member, IEEE "Distributed Denial of Service Prevention Techniques" International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010, pp 268-276.

[28] Lohit Kapoor, Seema Bawa, Ankur Gupta "Detecting Containing Malicious Services in an intercloud environment" International Journal of web engineering Vol. 1, No. 1, 2016 pp 1-19.

[29] Karnwal, T., S. Thandapanii, and A. Gnanasekaran, A Filter Tree Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS Attack. Intelligent Informatics.

[30] Neustar Annual DDoS Attacks and protection Report april 2016. https://www.neustar.biz biz/neustar/www/resources/whitepapers/it-security/ddos/2016-apr-ddos-report.pdf.