ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

A Survey on Economic Denial of Sustainability Attack Mitigation Techniques

Rohit Thaper[1], Amandeep Verma[2]

Research Scholar, Dept. of IT, U.I.E.T., PU, Chandigarh, India[1]

Assistant Professor, Dept. of IT, U.I.E.T., PU, Chandigarh, India[2]

ABSTRACT: Cloud computing is most widely used current technology. It provides a higher availability of resources to greater number of end users. Cloud computing provides rich computing platforms which utilizes the resources on the basis of 'pay-per-use' model. This model automatically scales the resources according to the demand of consumers. This functionality of this model is to mitigate the EDoS attack by some tactical attacker/s, group of attackers or zombie machine network (BOTNET) to minimize the availability of the target resources, which directly or indirectly reduces the profits and increase the cost for the cloud operators. This paper reviews different possible attacks on the cloud and methods to mitigate certain attacks like DoS, DDoS, EDoS, etc.

KEYWORDS: Ehanced EDoS shield, cloudwatch, cloud attacks, EDoS shield, EDoS mitigation techniques, etc.

I. INTRODUCTION

Currently Cloud computing is becoming the most important topic in information technology. Cloud computing has the ability to provide a number of services to the end users. It delivers resources over the internet. Cloud computing provide processing power, Data storage and networks to the user application [1]. Cloud computing in a model comprising of information processing, information storage and delivery of physical resources to the clients on demand. There are a number of attacks in the cloud computing. One of the main attack is Denial-of-service which crashes the server by creating miscommunication among the users.

Denial-of-service (DoS) is a destructive attack to online servers. This attack minimizes the possibility of a host, router or entire network. They establish a number of computation tasks or sends a large amount of unwanted packets to burden the system. It results as a serious damage to the services running on the host therefore some detection method of DOS attack is necessary to protect the online services [2].

DoS attacks can either be from a single source or from a number of sources. Distributed denial-of-service (DDoS) is an attack that originates from multiple sources and it is very hard to detect. In this attack a large amount of valid packets are send from multiple attacks sides to crush the server. As a result the victim uses its main resources for the attack packets and unable to attend its valid clients. During these attacks, DoS traffic also creates a heavy congestion in the internet core which disturbs the communication between all the users of internet [3].

Economic denial-of-sustainability (EDOS) is a type of attack that makes use of available resources, raises the cost thus resulting in profit decrement in order to make it unable to sustain its life of the service provider to sustain services for the user in future. An EDoS attack occurs when a zombie machine sends a very large amount of unwanted traffic to the cloud and uses the scalability of cloud. As a result, this attack makes the cloud unsustainable by charging the bill of user for activities of the attack [4].

As shown in fig. 1[5] the botnets are widely used to launch the DDoS attacks. The botnets are the networks of the zombie nodes and botnet master nodes, which are centrally controlled by one botnet master. The zombie nodes are the slave nodes, which are the normal user computers deployed with the remotely operated malware tools. These malware tools takes the command from the botnet master and act accordingly. The botnet master when commands the zombie nodes to launch the DoS traffic streams towards the given target node, which collectively results as the DDoS attack [6].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

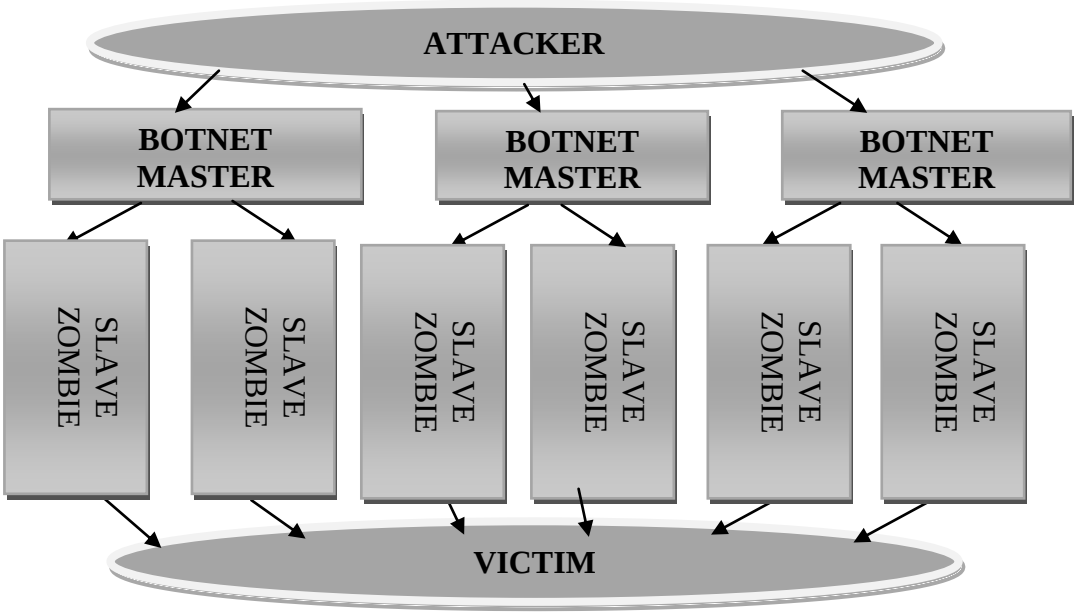

Figure .1 Block diagram of DDoS attack.

II. RELATED WORK

Mitigation techniques are used to protect the cloud framework from the various attacks. Mitigation techniques for DoS attacks mainly comprises of four steps- Prevention, Detection, Tracking and Suppression [7]. The flow of these steps are represented in fig.2

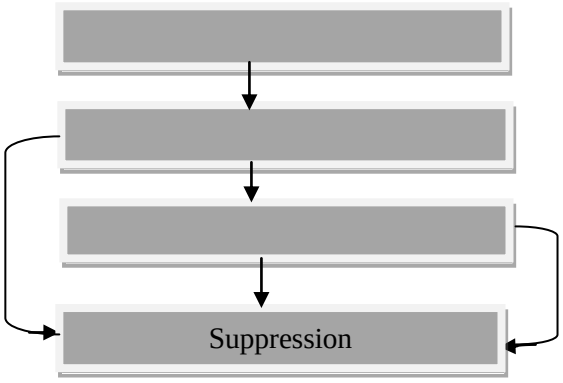

Figure 2. Steps of DoS attack mitigation

In this section we will discuss the main mitigation techniques for EDoS attacks.

CloudWatch [8] is an auto scaling technique to prevent EDoS attacks introduced by Amazon as a control technology. CloudWatch is a service that monitors cloud resources with the help of which the clients can define the boundaries of the cloud and it helps to limit the elasticity of the cloud platform as a result the effect EDoS can be reduce.

Another mitigation technique for EDoS introduced by HinKhor and Nakao[9] is sPoW (self-verifying proof of work) in this technique the server demands a proof of work from the client side, before committing its resources, clients uses their resources to solve "crypto-puzzle" and finally submit a proof of the solution to the server. sPoW which helps the clients to communicate with the protected server, has to verify the correctness of the puzzle and giving priority to the various requests based on the difficulty level of puzzle. As a result, the number of application level EDoS connection request are reduced which in turn reduces the effect of EDoS attack.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Mohammad H.Sqalli and Fahd Al-Haidari [10] proposed a technique to prevent EDoS attacks named as EDos shield as shown in fig. 3. The architecture of this technique has two main components: verifier cloud nodes (V-Nodes) and virtual firewalls (VF). The virtual firewall consists black and white lists. A white list contains the authenticated source IP addresses so that the firewall allow the traffic coming from these sources to pass towards the destined services and black lists contains the IP addresses of all unauthenticated sources so that the traffic coming from these sources are not allowed to pass through the firewall. These lists are needed to update periodically. Therefore a verifier node is used which changes the lists on the basis of the verification process. This technique is considered as an effective approach on the basis of its cost and performance metrics.

In [11], an enhanced EDoS-shield is proposed which Mitigates EDoS attack. They use the time to live (TTL) parameter of the IP packet header field for calculating the maximum life time of packet inside the network value of TTL is decremented each time when packet passes through any router. The packet will be discarded whenever TTL value becomes zero. This prevents infinite looping of packet in the network.

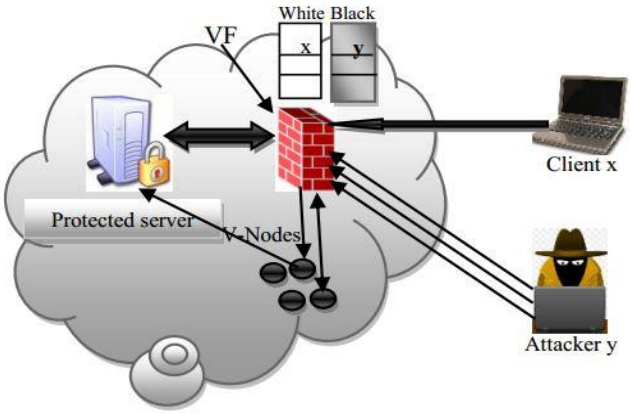

Figure. 3. The Proposed EDoS-Shield Architecture for mitigating EDoS.

In [12] A Framework to encounter EDoS by testing the first packet from the source of request to established legitimacy of the source using a Graphical Turing Test (GTT) is proposed. In this method source of first packet receive at firewall is checked against the existing list to verify the source node. If source IP does not found in the list then that packet will be forwarded to verifier node. Further verifier node sends a GGT test to the user. If user passes the test a positive acknowledgment is sent to the firewall and packet is verified as legitimate. Otherwise a negative acknowledgment is received at the firewall and packet is refused. Also IP address of source will be added to blacklist considering it as a malicious packet. This proposed scenario implemented an efficient filtering system against the DDoS which replaces the location hiding of the protected servers by reverse proxy method. This function also helps in other tasks such as load balancing.

S.no	AUTHOR NAME AND YEAR	PROBLEM ADDRESSED	PROPOSED SOLUTION	RESULTS	OUR REVIEW
1.	HinKhor and Nakao[2006]	Reduction of Number of application-level EDoS connection requests.	sPoW (self-verifying proof of work)	The number of application level EDoS connection request are reduced which in turn reduces the effect of EDoS attack.	Protects against application level EDoS attacks. But does not offer any protection against the EDoS attacks on the Entry points.
2.	Mohammad H.Sqalli and Fahd Al-Haidari[2011]	Direct source DDoS and EDoS attack	EDos shield	Technique is considered as an effective	EDoS protects against the direct source EDoS

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

				approach on the basis of its cost and performance metrics.	attacks only. This scheme is prone to spoofed IP based EDoS attack.
3.	F.Al-Haidari,M.H.Sqalli and Khaled Salah[2012]	Spoofed-IP based DDoS and EDoS attack	Enhanced EDoS-shield	Prevents infinite looping of packet in the network.	Protect against Spoofed IP based EDoS attacks. But does offer protection against the patronized DDoS attacks from multiple sources.
4.	AMAZON INC. [2012]	Direct source DDoS and EDoS attack.	Cloud Watch auto scaling technique.	Limit the elasticity of the cloud platform as a result the effect EDoS can be reduce.	CloudWatch protects against the direct source EDoS attacks only. This scheme is prone to spoofed IP based EDoS attack.
5.	Wael Alosaimi and Khalid Al-Begain[2013]	EDoS attack prevention by ensuring the legitimate users	Scenario of testing the first packet	Efficient filtering system against the DDoS which replaces the location hiding of the protected servers by reverse proxy method.	Ensures the entry of legitimate users, But does not protect against the internals attacks.

Table. 1. Comparison of different mitigation techniques.

III. CONCLUSION AND FUTURE WORK

In this paper, we have conducted the survey on the prevention schemes EDoS attacks. The existing EDoS prevention techniques has been evaluated for their nature of protection and the mechanism used for the protection shield. The existing schemes have been designed to protect the various types of EDoS or DDoS attacks such as direct source EDoS, Spoofed-IP based EDoS, application-level EDoS, etc. Under this survey, we have evaluated the effectiveness of their protection hardness against the EDoS and DDoS attacks. The Enhanced EDoS shield has been found the best mechanism to protect against the EDoS attack on the cloud platforms. The cloud platforms have been made well protected against the various forms of EDoS attack (such as Spoofed IP based EDoS, Direct EDoS, application-level EDoS, etc.) using the Enhanced EDoS shield. Whereas the Enhanced EDoS shield has been found ineffective and non-programmed to protect the supervised and controlled output based EDoS attacks launched from various sources. Such attacks are known as the silent killers and does not get detected by the ordinary traffic analysers.

In the future, the Ehanced EDoS shield will be improved in order to protect against the EDoS attacks based on supervised and controlled output manner. Also, the enhanced EDoS shield would be tested for more vulnerabilities. If more vulnerability would be found, they would also take into account for the improvement in the enhanced EDoS shield EDoS prevention mechanism.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

REFERENCES

1. [online] http://csrc.nist.gov/groups/SNS/cloud-computing/.
2. Z.Tan, A.Jamdagni, and X. He, "A System for Denial-of-Service Attack Detection based on Multivariate Correlation Analysis," IEEE Transactions on parallel and distributed systems, vol., no., 2013, pp. 1-10.
3. N.H.Bhandari, Survey on DDoS Attacks and its Detection & Defence Approaches, ISSN:2319-6386., vol. 1,Issue. 3,February 2013, pp.67-71.
4. Al-Haidari,M.Sqalli,K.Salah,'Evaluation of the Impact of EDoS Attacks Against Cloud Computing Services',In:Arab.J.Sci Eng(Springer),pp 1-13.
5. [online]http://www.ijarcsse.com/docs/papers/9_September2012/Volume_2_issue_9/V2I900121.pdf.
6. [online]http://www.incapsula.com/ddos/ddos-attacks/botnet-ddos.html.
7. [online]http:/www-lor.int-evry.fr/~paul_0/Courses/ddos/pdf.
8. "Amazon CloudWatch", Amzon Website, available at http://aws.amazon.com/cloudwatch/.
9. S. HinKhor and A. Nakao, "sPoW: On-Demand Cloud-Based eDDoS Mitigation Mechanism", HotDep (Fifth Workshop on Hot Topices in System Dependability), Lisbon, Portugal,2009.
10. Sqalli, M.; Al-Haidari, F.; Salah, K.: EDoS-Shield—a two-steps mitigation technique against EDoS attacks in cloud computing.In: Fourth IEEE International Conference on Utility and Cloud Computing (UCC 2011), Victoria, NSW, pp. 49–56 (2012).
11. Al, F., Sqalli, M., AND Salah, K., 2012. Enhanced EDoS-Shield for Mitigating EDoS Attacks Originating from Spoofed IP Addresses. *In 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communicvations* IEEE, pp.1167-1174
12. W. Alosaimi and K., Al-Begain, " An Enhanced economical Denial of Sustainability Mitigation System for the Cloud", IEEE@2013, pp1-7.