Moving Target Defense Strategy for Mitigating Denial of Service Attack in the Public Cloud Environment

Gayathri RajaKumaran, Neelanarayanan Venkataraman

***Abstract:** Internet is a network of interconnected systems which works collaboratively and services the users without any disruption. But for achieving the same in real time, needs the new prominent technology cloud computing. The massive attractive features and simple pay-as-you-go model of cloud makes it reachable to all the users Denial-of-Service (DoS) plays a crucial role in making the services inaccessible to its intended users. The traditional DoS can no longer be successful in the cloud scenario as it poses the auto scaling feature. Still, the DoS can consume the bandwidth of the cloud customers as they need to pay for their complete usage. In spite of the huge number of recovery measures available in cloud, DoS becoming harder every day in terms of attack volume and severity. Hence complete mitigation against DoS attack is the expected solution which needs to be proved in today's digital world. Moving Target Defence (MTD) is one such prominent emerging solution which aims to avoid the DDoS attacks in the cloud environment. The challenge of MTD is to change the attack surface periodically such that the attackers will be facing difficulty in even the attack attempts. This paper aims to provide solution for avoiding DoS attack by adopting MTD algorithm for making the web servers redundant in the cloud environment. Experimental simulations prove the effectiveness of MTD in the public cloud environment.*

***Index Terms**: DDoS, Moving Target Defense, public cloud*

I. INTRODUCTION

Cloud computing is the technology of making the resources available to its intended users on-demand without any direct user intervention. In addition, large volume of resources is pooled in cloud to serve customers without any service disruption and unavailability. It helps greatly in reducing the delay in accessing the services too. Security attacks emerge every day with advancements in the technology developments and disrupt the privacy, integrity and availability of services offered to the customers. Out of other security attack, Denial of Service attack (DoS) consumes the bandwidth of cloud customers by flooding the servers with bogus requests. In cloud, complete service cannot be denied to the users but consumption of bandwidth by the bogus requests makes the users to pay more than their actual usage. More solutions exist in the literature for the process of detection and prevention of DoS attacks in the cloud environment and we have anti-DoS solution too offered by the Cloud Service Provider (CSP). In spite of the numerous cloud-based DoS solutions, our focus is to find prominent solution for avoiding the DDoS attack in the cloud computing environment preferably public cloud which is discussed detail in the following sections.

II. RELATED WORK

Numerous works focus on the detection and prevention of Denial of Service attacks in the cloud environment. The solution starts from Firewalls, Intrusion Detection System, Intrusion Prevention Systems and cloud-based anti-DoS. But effectiveness against DoS attacks remains to be challenging and none of them offers a complete protective shield for avoiding such attacks. For avoiding the DoS attacks, the emerging solution is the Moving Target Defense (MTD) in various fields which is discussed detail in our literature review.New prominent solutions are required for DoS as the defects in system design and vulnerabilities are unavoidable due to the limitations of the human's cognitive approaches. The MTD is the revolutionary technique which tries to create a conductive network environment for defence by increasing the attacker's apparent uncertainty. The moving target is widely applied in many fields such as Biology, cryptography and military [1][2][3]. The evaluation architecture of MTD are based on change-point detection, activity templates and quantification framework [5][6][7]. Hidden Moving Target Defence approach [8] is proposed which cannot be detected by the attackers meanwhile it helps to maintain power flow to the grid. Stealthy and completeness are the two major goals considered in the MTD design. The operational costs of MTD are also discussed under the dc and ac models. Simulations are done to show the effectiveness of the hidden MTD against the false data injection attacks under realistic settings. The Denial of Service scenario is formulated as a two-player game and the problem is solved using the empirical game-theoretic analysis [10]. The performance strategies and solution effectiveness are validated through the agent-based simulation methods. The strategic stability of various categories like proactive server movement, delayed attack timing and suspected insider blocking are blocked effectively through the concepts of MTD.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

Gayathri Rajakumaran*, School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, India.
Neelanarayanan Venkataraman, School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, India.

Retrieval Number F8077088619/2019©BEIESP
DOI: 10.35940/ijeat.F8077.088619
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

New client-to-proxy assignment strategy [11] is proposed which employs MTD which helps in isolating the compromised clients thereby reduces the impact of attacks. The experiment is validated both theoretically and through simulations which limits effectively the number of proxies discovered by an attacker and isolates malicious clients.

MOTAG method [12] has been proposed for combating DDoS attacks in the cloud environment. This method of Moving Target Defense to overcome DDoS attacks will frequently shuffle the requests between client to server for identifying malicious clients and quarantining them. This in turn addresses the challenge of creating DDoS detection and mitigation system to achieve protection against volumetric and resource-specific starvation and exhaustion attacks.

Various MTD techniques are proposed in different domains but properly assessing and evaluating their efficiency is important. Hierarchical Attack representation model [13] is the security model to evaluate the effectiveness of MTD. Importance Measures (IMs) are used for employing MTD techniques in order to enhance the concept of scalability. Hierarchical and attack graph representation models are compared in terms of scalability. System Attack Surface (SAS) model [14] is proposed to demonstrate how the system resources are affected during attack cases. Hierarchical Hidden Markov model is used to find all possible states of attack sequences by introducing the partial Viterbi algorithm. The attacking states handled by Moving Target (MT) adversaries and system cost increase during reconfiguration is also discussed. To prevent the closing cluster attack, server redundancy and rotations [26] are achieved through the Moving Target defense measure which helps greatly in increasing the serviceability and availability constraint of servers which aims to offer completely protection form the closed cluster attacks.

III. NEED FOR MOVING TARGET DEFENSE

Defects during the system design phase [9] cannot be avoided due to the limitations in human cognitive approaches. Hence it poses a loophole which in turn exploited by the hackers for system compromise and various other attack categories. In general, actions of hackers are intrusion which disturbs the legitimate users in accessing service. The various activities done by hackers to gather system information before launching any attack are listed as below

i) Gather information about the network

ii) Analyse network features

iii) Formulate attack tools and methods

Through structure remodelling and system defence remodelling, such information gathering by hackers would be reduced. This kind of methods can invalidate the attacks related to specific vulnerability exploitation. As it is difficult for the hackers to launch attacks without exploiting the vulnerabilities. In this context, the system security is improved and it will be impractical to remodel the complete system. This is the role of the Moving Target Defence. Making a target difficult to achieve by the hackers as we are changing the target in terms of remodelling.

IV. MTD KEY ASPECTS

The MTD key aspect procedure can be classified into three categories which is illustrated as below

1. Shuffle
2. Diversity
3. Redundancy

Shuffle:

The technique of shuffle is to rearrange the various system specific settings to various layers such as randomizing the address [15][16][17][18], migration or other topology arrangements.

Diversity:

This technique provides equivalent functions for various implementations such as operating systems and variant software stack components [19][20][21][22].

Redundancy:

The technique of redundancy is to provide multiple replicas [23][24][25] for various categories of network components such as the offered services, nodes in the network or paths. These methods also could be combined for enriching the security mechanisms.

V. PROPOSED EXPERIMENTAL SET UP

In our work, we have considered redundancy aspect for securing the web servers from Denial of Service attack with respect to the public cloud environment. The test bed for simulation is the Amazon Web Services (AWS) console with the intention of providing maximum performance and availability of web servers in delivering the services. We denote the number of replicas as 'r' for an 'n' number of replications. Redundancy testing is done under two scenarios 1) performance analysis and 2) security analysis. We assume that each web server is provided with 3 replicas and all VM's are running the same Operating System (OS).

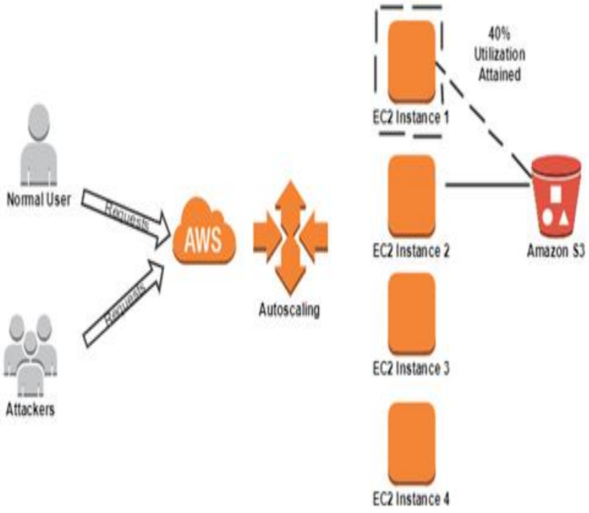

Fig 1: MTD redundancy technique for web server in AWS

The above Fig 1 demonstrates the experimental set up of applying MTD redundancy technique in the AWS console. The legitimate and normal traffic requests are simulated and the DoS identification is done through the Simple Network Management Protocol (SNMP) [26] [27]. From the references, it is evident that SNMP is effective in identifying DDoS attacks in AWS and the same has been validated experimentally. For enhancing the performance of web servers and making the target difficult to reach for the attacker, 4 Elastic Cloud Computing (EC2) instances are created, out of which 3 are assumed as replicas for the EC2 instance 1 (web server). When the EC2 instance 1 attains the CPU utilization of 40%, all the incoming requests are routed to the replicas and the storage Amazon S3 is linked to the current EC2 instance which is providing service. It is also evident that a system with an enabled MTD strategy is effective against a reconnaissance attack because the random changes in the system orchestrated by the MTD strategy will invalidate the information that the attackers previously obtained. All the EC2 instances are monitored and alarm will be triggered when the utilization reaches 40%.

VI. METHODOLOGY ADOPTED

The Moving Target Defense category applied in our proposed methodology is redundancy through various defense measures and changing services periodically in the chosen Virtual Machines (VM's). 3 Identical VM's (referred as backup VM's) are created to handle the services of the original web server VM. The CPU utilization is the metric chosen to route the service requests to the backup VM's. Each backup VM is configured with different DoS mitigation strategies as it should not provide any guess to the attackers about the prevention measures adopted. In order to avoid the exploits during the reconnaissance, the service offered by the web server is routed to backup VM's under threshold condition in order to make the DoS attack harder to launch. The results obtained through our experimental test bed in AWS are illustrated as below. The prevention measures against DDoS used Simple Network Management Protocol (SNMP) and HTTP server parsing. The web server doesn't employ any DDoS prevention measures and once the CPU utilization of 40% is reached, all the incoming requests are routed to the back up VM's. The DoS prevention strategies are employed only in the backup VM's.

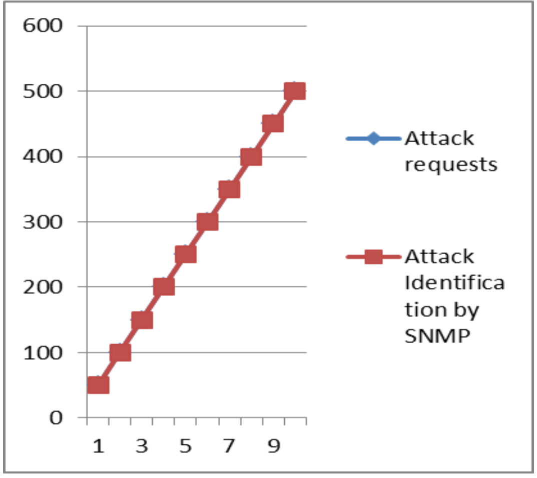

Fig 2: Attack Identification in VM1 using SNMP

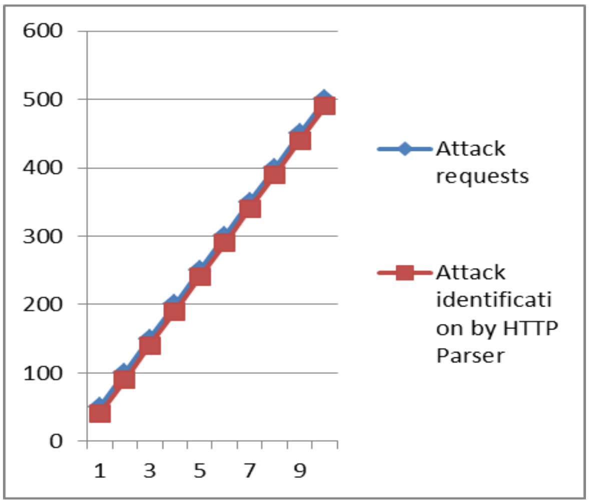

Fig 3: Attack Identification in VM2 using HTTP Parser

The above Fig 2 and Fig 3, illustrates the effectiveness of attack identification methods used in the VM's in an experimental test bed. The VM1 employs the SNMP mitigation strategy which is achieved through the SNMP MIB variables [27] specific to DoS attacks and achieves 99.9% accuracy in the attack detection process. The VM2 employs HTTP parsing as it validates and verifies the header of all incoming traffic flows and differentiates normal flow with the attack flow. In the cases, where the attack flow tools are using techniques to make the packet appear as the normal one, hence it is effective in detecting the DoS attacks by 93%.

VII. RESULTS AND DISCUSSION

Through our experiments, it is evident that our adopted mitigation measures are effective in preventing DoS attack as represented below.

SL.No	Mitigation Measure	Accuracy
1	SNMP MIB Variables: tcpAttemptFails tcpCurrEstab tcpOutRsts	99.7%
2	HTTP Parser	90%

I Detection Measures Accuracy

The prevention measures are employed through the Moving Target Defense strategy in order to obtain extra layer of protection and to attain prevention from the reconnaissance phase during the attack scenario. The proposed Moving Target Defense strategy for achieving redundancy in web servers in the Amazon Web Services (AWS) console satisfies the performance constraints of web services. The obtained results proves the automatic switching and routing of web server requests to the EC2 instance replicas effectively and services all the incoming normal user requests. All the intrusive or Distributed Denial of Service (DDoS) attack requests are identified and blocked using the Simple Network Management Protocol (SNMP) and HTTP Parsing. Hence only the normal requests are serviced by all the EC2 replicas. This method further helps in reducing the possibility of DDoS attack against the EC2 instances as we are routing the user requests to EC2 instances periodically.

The future scope focusses on the complete performance evaluation of the MTD redundancy technique and assessing the effectiveness of the same through the security models.

REFERENCES

1. D. Kramer and W. Karl, "Realizing a proactive, self-optimizing system behavior within adaptive, heterogeneous many-core architectures," in Proceedings of the 2012 IEEE 6th International Conference on Self-Adaptive and Self-Organizing Systems, SASO 2012, pp. 39–48, France, September 2012.
2. R. Nee and R. Prasad, OFDM for Wireless Multimedia Communications, Artech House, Inc, 2000.
3. H. Zhang G, L. C. Li, and M. Tang, "Capability of evolutionary cryptosystems against differential cryptanalysis," SCIENTIA SINICA Informationis, vol. 43, no. 4, pp. 545–554, 2013.
4. https://zeltser.com/reasons-for-denial-of-service-attacks/
5. [116] K. Zaffarano, J. Taylor, and S. Hamilton, "A quantitative framework for moving target defense effectiveness evaluation," in Proceedings of the 2nd ACM Workshop on Moving Target Defense, MTD 2015, pp. 3–10, USA.
6. C.Lei, D.-h.Ma, H.-q. Zhang, and L.-m.Wang, "Moving target network defense effectiveness evaluation based on change-point detection," Mathematical Problems in Engineering, vol. 2016, Article ID 6391502, 11 pages, 2016.
7. J. Taylor, K. Zaffarano, B. Koller, C. Bancroft, and J. Syversen, "Automated effectiveness evaluation of moving target defenses: metrics for missions and attacks," in Proceedings of the 2016 ACMWorkshop on Moving Target Defense, MTD 2016, pp. 129–134, Austria.
8. Jue Tian , Rui Tan, Xiaohong Guan and Ting Liu, " Enhaced Hidden Moving Target Defence in Smart Grids", IEEE Transactions on Smart Grid, Vol:10(2), pp.2208-2223, March 2019.
9. Cheng Lei , Hong-Qi Zhang, Jing-Lei Tan,Yu-Chen Zhang and Xiao-Hu Liu, " Moving Target Defense Techniques: A Survey", Hindawi, Security and Communication Networks, Vol:2018, https://doi.org/10.1155/2018/3759626.
10. Mason Wright, Sridhar Venkatesan, Massimiliano Albanese and Michael P. Wellman, "Moving Target Defense against DDoS attacks: An Empirical Game-Theoretic Analysis", Proceedings of the 2016 ACM workshop on Moving Target Defense, pp.93-104, 2016.
11. Sridhar Venkatesan, Massimiliano Albanese, Kareem Amin, Sushil Jajodia and Mason Wright, " A Moving Target Defense Approach to Mitigate DDoS Attacks against Proxy-Based Architecture", IEEE conference on Communications and Network Security (CNS), 2016.
12. Kesavamoorthy R, Thangamariappan L and Ruba Soundar K, "Securing cloud computing environment by mitigating DDoS attacks: Moving target defense approach", http:www.alliedacademies.org/advanced-materials-science-research, 2017.
13. Jin B. Hong and Dong Seong Kim," Assessing the Effectiveness of Moving Target Defenses Using Security Models", IEEE Transactions on Dependable and Secure Computing, Vol:13(2), pp.163-177, April 2016.
14. XIN-LI XIONG, LIN YANG and GUANG-SHENG ZHAO, Effectiveness Evaluation Model of Moving Target Defense Based on System Attack Surface", IEEE Access, Digital Object Identifier 10.1109/ACCESS.2019.2891613, 2019.
15. J. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: Transparent moving target defense using software defined networking," in Proc. Hot Topics Softw. Defined Netw., 2012, pp. 127–132.
16. S. Antonatos, P. Akritidis, E. Markatos, and K. Anagnostakis, "Defending against hitlist worms using network address space randomization," in Proc.ACMWorkshop Rapid Malcode, 2005, pp. 30–40.
17. B. Danev, R. Masti, G. Karame, and S. Capkun, "Enabling secure VM-vTPM migration in private clouds," in Proc. 27th Annu. Comput. Security Appl. Conf., 2011, pp. 187–196.
18. Y. Zhang, M. Li, K. Bai, M. Yu, and W. Zang, "Incentive compatible moving target defense against VM-colocation attacks in clouds," in Information Security and Privacy Research, vol. 376, series IFIP Advances in Information and Communication Technology, D. Gritzalis, S. Furnell, and M. Theoharidou, Eds. New York, NY,
19. USA: Springer, 2012, pp. 388–399.
20. J. Rohrer, A. Jabbar, and J. Sterbenz, "Path diversification for future internet end-to-end resilience and survivability," Telecommun. Syst., vol. 56, pp. 49–67, 2014.
21. A. Newell, D. Obenshain, T. Tantillo, C. Nita-Rotaru, and Y. Amir, "Increasing network resiliency by optimally assigning diverse variants to routing nodes," in Proc. 43rd Annu. IEEE/IFIP Int. Conf.Dependable Syst. Netw., 2013, pp. 1–12.
22. D. Glynis, H. Salim, A. Youssif, and R. Gabriel, "Resilient dynamic data driven application systems (rDDDAS)," Procedia Comput. Sci., vol. 18, pp. 1929–1938, 2013.
23. T. Jackson, B. Salamat, A. Homescu, K. Manivannan, G. Wagner, A. Gal, S. Brunthaler, C. Wimmer, and M. Franz, "Compiler-Generated software diversity," in Moving Target Defense, vol. 54, series Advances in Information Security, S. Jajodia, A. K. Ghosh,
24. V. Swarup, C. Wang, and X. S. Wang, Eds. New York, NY, USA: Springer, 2011, pp. 77–98.
25. H. Kirrmann and D. Dzung, "Selecting a standard redundancy method for highly available industrial networks," in Proc. 3rd IEEE Int. Workshop Factory Commun. Syst., 2006, pp. 386–390.
26. S. Al-Wakeel and S. A. Al-Swailemm, "PRSA: A path redundancy based security algorithm for wireless sensor networks," in Proc. IEEE Wireless Commun. Netw. Conf., Mar. 2007, pp. 4156–4160.
27. E. Yuan, S. Malek, B. Schmerl, D. Garlan, and J. Gennari, "Architecture-based Self-protecting software systems," in Proc. 9th Int. ACM Sigsoft Conf. Quality Softw. Archit., 2013, pp. 33–42.
28. Y. Huang, D. Arsenault, and A. Sood, "Closing cluster attack windows through server redundancy and rotations," in Proc. 6th IEEE Int. Symp. Cluster Comput. Grid, May 2006, vol. 2, pp. 12–21.
29. Rajakumaran Gayathri and Venkataraman Neelanarayanan, "Simulation and analysis of DoS attack in cloud Environment", Int. J. Knowledge Engineering and Soft Data Paradigms, Vol. 6, No. 1, 2017.
30. Gayathri R and Neelanarayanan V, "DoS detection solution for cloud platform using SNMP", International Journal of Pure and Applied Mathematics, vol.119 (11), pp-175-183, 2018.

AUTHORS PROFILE

Gayathri Rajakumaran received her B.Tech (CSE) from Rajiv Gandhi College of engineering and technology and M.Tech from Pondicherry Engineering College in the year 2011, Puducherry. She is currently employed at VIT University Chennai campus as Assistant Professor in the department of Computing Science and Engineering. Her research interests include cloud computing, information security and network security.

Neelanarayanan Venkataraman is an Associate Professor in the School of Computing Science and Engineering, VIT University, Chennai, India. He received PhD in Computer Science, 2007 from IT University of Copenhagen, Denmark. His research interests are Distributed Computing, Cloud Computing, Grid Computing, Network Management and Security, Context - Aware Computing.