International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Denial of Service Strategy Over Outsourced Encrypted Data in Cloud Computing

S. Lakshmi Prasanna, P. V. Ramesh
Department of Computer Applications, Rayalaseema Institute of Information and Management Sciences, Tirupathi, Andhra Pradesh, India

ABSTRACT

The success of the Cloud Computing paradigm is because of its on-demand, self-service, and pay-by-use nature. According to this paradigm, the results of Denial of Service (DoS) attacks involve not solely the standard of the delivered service, but conjointly the service maintenance prices in terms of resource consumption. Specifically, the longer the detection delay is, the higher the prices to be incurred. Therefore, a specific attention has to be got concealed DoS attacks. They aim at minimizing their visibility, and at identical time, they'll be as harmful as the brute-force attacks. they're refined attacks tailored to leverage the worst-case performance of the target system through specific periodic, pulsing, and low-rate traffic patterns. In this paper, we have a tendency to propose a technique to orchestrate concealed attack patterns, that exhibit a slowly-increasing-intensity trend designed to intercommunicate the utmost monetary value to the cloud customer, whereas respecting the duty size and therefore the service arrival rate obligatory by the detection mechanisms. we describe each how to apply the projected strategy, and its effects on the target system deployed within the cloud.

Keywords: Cloud Computing, sophisticated attacks strategy, low-rate attacks, intrusion detection.

I. INTRODUCTION

Cloud Computing is an emerging paradigm that enables customers to get cloud resources and services in step with an on-demand, self-service, and pay-by-use business model. Service Level Agreements (SLA) regulate the prices that the cloud customers have to be compelled to acquire the provided Quality of Service (QoS). A facet impact of such a model is that, it's prone to DoS and Distributed DoS (DDoS), that aim at reducing the service availableness and performance by exhausting the resources of the service's host system;including memory, processing resources, and network bandwidth. Such attacks have computer graphics within the cloud as a result of the adopted pay-by-use business model. Specifically, in Cloud Computing conjointly a partial service degradation as a result of an attack has direct impact on the service prices, and not solely on the performance and availableness perceived by the client. The delay of the cloud service provider to diagnose the causes of the service degradation (i.e., if it's as a result of either an attack or an overload) is considered as a security vulnerability. It is exploited by attackers that aim at exhausting the cloud resources (allocated to satisfy the negotiated QoS), and seriously degrading the QoS, as happened to the BitBucket Cloud, that went down for 19h. Therefore, the cloud management system needs to implement specific countermeasures so as to avoid paying credits just in case of accidental or deliberate intrusion that cause violations of QoSguarantees.Over the past decade, several efforts are dedicated to the detection of DDoS attacks in distributed systems. Security prevention mechanisms typically use approaches supported ratecontrolling, time-window, worst-case

threshold, and patternmatching methods to discriminate between the nominal system operation and malicious behaviors. On the opposite hand, the attackers are alert to the presence of such protection mechanisms. They arrange to perform their activities in an exceedingly "stealthy" fashion so as to elude the protection mechanisms, by orchestrating and temporal arrangement attack patterns that leverage specific weaknesses of target systems. They're meted out by directing flows of legitimate service requests against a selected system at such a low-rate that may evade the DDoS detection mechanisms, and prolong the attack latency, i.e., the number of time that the continued attack to the system has been unseen. In this paper, we propose a in public verifiable dynamic searchable radial encoding scheme supported the buildup tree. we tend to 1st construct an accumulation tree supported encrypted knowledge and so source both of them to the cloud. Next, throughout the search operation, the cloud generates the corresponding proof in step with the question result by mapping mathematician question operations to line operations, while keeping privacy-preservation and achieving the verification requirements: freshness, legitimacy, and completeness. Finally, we extend our theme by dividing the buildup tree into different tiny accumulation trees to form our theme ascendible. The security analysis and performance analysis show that the proposed theme is secure and sensible. This paper presents a complicated strategy to orchestrate stealthy attack patterns against applications running within the cloud. rather than aiming at creating the service inaccessible, the proposed strategy aims at exploiting the cloud flexibility, forcing the application to consume a lot of resources than required, affecting the cloud client a lot of on money aspects than on the service availableness. The attack pattern is musical organization in order to evade, or however, greatly delay the techniques proposed within the literature to discover low-rate attacks. It does not exhibit a periodic undulation typical of low-rate exhausting attacks. In distinction with them, it is an iterative and progressive method. specially, the attack potency (in terms of service requests rate and coincident attack sources) is slowly increased by a patient offender, so as to inflict vital money losses, even though the attack pattern is performed in accordance to the utmost job size and arrival rate of the service requests allowed within the system. Using a simplified model through empirical observation designed, we tend to derive an expression for bit by bit increasing the efficiency of the attack, as a function of the reached service degradation (without knowing in advance the target system capability). we tend to show that the features offered by the cloud supplier, to confirm the SLA negotiated with the client (including the load equalizationand auto-scaling mechanisms), is maliciously exploited by the planned lurking attack, that slowly exhausts the resources provided by the cloud supplier, and will increase the costs incurred by the client. The planned attack strategy, specifically SIPDAS (Slowly-Increasing-Polymorphic DDoS Attack Strategy) is applied to several reasonably attacks, that leverage famed application vulnerabilities, so as to degrade the service provided by the target application server running within the cloud. The term polymorphic is galvanized to polymorphic attacks that amendment message sequence at each sequent infection so as to evade signature detection mechanisms. Even though the victim detects the SIPDAS attack, the attack strategy is re-initiate by employing a completely different application vulnerability (polymorphism in the form), or a special temporal arrangement (polymorphism over time).

II. ALGORITHM

DDoS attack pattern in the cloud the purpose of the attack against cloud applications is not to necessarily deny the service, but rather to inflict significant degradation in some aspect of the service (*e.g.*, service response time), namely *attack profit PA*, in order to maximize the cloud resource consumption CAto process malicious requests. In order to elude the attack detection, different attacks that use low-

rate traffic (but well orchestrated and timed) have been presented in the literature. Therefore, several works have proposed techniques to detect low-rate DDoS attacks, which monitor anomalies in the fluctuation of the incoming traffic through either a time- or frequency-domain analysis. They assume that, the main anomaly can be incurred during a low-rate attack is that, the incoming service requests fluctuate in a more extreme manner during an attack. The abnormal fluctuation is a combined result of two different kinds of behaviors: (*i*) a periodic and impulse trend in the attack pattern, and (*ii*) the fast decline in the incoming traffic volume (the legitimate requests are continually discarded).

Denote π the number of attack flows, and consider a time window T, the DDoS attack is successful in the cloud, if it maximizes the following functions of profit and resource consumption:

$$\textit{maximize} \quad P_A = \sum_{j=1}^{\pi} \sum_i g(\varphi_{j,i}),$$
$$\textit{maximize} \quad C_A = \sum_{j=1}^{\pi} \sum_i w(\vartheta_{j,i}),$$

and it is performed in stealthy fashion, if each flow ϕAj satisfies the following conditions:

$$\begin{array}{ll} \textit{minimize} & \delta_j, \quad \forall j \in [1..\pi], \\ \textit{s.t. to} & \varphi_{j,i} \in \theta, \\ \textit{s.t. to} & \textit{exhibits a pattern neither periodic} \\ & \textit{nor impulsive}, \\ \textit{s.t. to} & \textit{exhibits a slowly increasing intensity}, \end{array}$$

where:

- ✓ gis the profit of the malicious request φj,i, which
- ✓ expresses the service degradation (e.g., in terms of increment
- ✓ of average service time tSto process the user
- ✓ requests with respect to the normal operation);
- ✓ δjis the average message rate of the flow ϕAj,
- ✓ w is the cost in terms of cloud resources necessary to processφj,i2 θ.

III. CONCLUSION

In this paper, we tend to propose a method to implement furtive attack patterns, that exhibit a slowly-increasing polymorphic behavior which will evade, or however, greatly delay the techniques proposed within the literature to notice low-rate attacks. Exploiting a vulnerability of the target application, a patient and intelligent wrongdoer will orchestrate subtle flows of messages, indistinguishable from legitimate service requests. In explicit, the projected attack pattern, rather than aiming at making the service unobtainable, it aims at exploiting the cloud flexibility, forcing the services to proportion and consume additional resources than required, poignant the cloud client additional on financial aspects than on the service convenience.

IV. REFERENCES

[1]. M. C. Mont, K. McCorry, N. Papanikolaou, and S. Pearson. Security and Privacy Governance in Cloud Computing via SLAs and a Policy Orchestration Service. In Proc. of the 2th Int. Conf. on Cloud Computingand Services Science, 2012, pp. 670-674.

[2]. F. Cheng and C. Meinel. Intrusion Detection in the Cloud. In Proc. Of the IEEE Int. Conf. on Dependable, Autonomic and Secure Computing, Dec. 2009, pp. 729-734.

[3]. C. Metz. DDoS attack rains down on Amazon Cloud. Available at: http://www.theregister.co.uk/2009/10/05/amaz on bitbucket outage/S, 26 Oct. 2009.

[4]. K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci. Robust and efficient detection of DDoS attacks for large-scale internet. In Computer Networks, vol. 51, no. 18, 2007, pp. 5036-5056.

[5]. H. Sun, John C. S. Lui, and D. K. Yau. Defending against low-rate tcp attacks: Dynamic detection and protection. In Proc. of the 12th IEEE Int.Conf. on Network Protocols, 2004, pp. 196-205.

[6]. A. Kuzmanovic and E. W. Knightly. Low-rate TCP-Targeted denial of service attacks: the shrew vs. the mice and elephants. In Proc. of the Int. Conf. on Applications, technologies, architectures, and protocols forcomputer communications, 2003, pp. 75-86.

[7]. M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang. Reduction of Quality (RoQ) Attacks on Internet End-Systems. In Proc. of the IEEE Int. Con.on Computer Communications (INFOCOM), pp. 1362-1372, Mar. 2005.

[8]. XiaodongXu, Xiao Guo, and Shirui Zhu. A queuing analysis for low-rate DoS attacks against application servers. In Proc. of the IEEE Int. Conf. onWireless Communications, Networking and Information Security, 2010, pp. 500-504.

[9]. Lanjia Wang, Zhichun Li, Yan Chen, Zhi Fu, Xing Li. Thwarting Zero- Day Polymorphic Worms With Network-Level Length-Based Signature Generation. In IEEE/ACM Transactions on Networking, 2010, pp. 53-66.

[10]. A. Chonka, Y. Xiang, W. Zhou, and A. Bonti. Cloud security defense to protect cloud computing against HTTP-DOS and XML-DoS attacks. In Journal of Network and Computer Applications, vol. 34, no. 4, July 2011, pp. 1097-1107.

[11]. D. Petcu, C. Craciun, M. Neagul, S. Panica, B. Di Martino, S. Venticinque, M. Rak, and R. Aversa. Architecturing a Sky Computing Platform. In Proc. of the Int. Conf. on Towards a service-based Internet, LNCS, vol. 6569, 2011, pp. 1-13.

[12]. U. Ben-Porat, A. Bremler-Barr, and H. Levy. Evaluating the Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks. In Proc. Of the IEEE Int. Conf. on Computer Communications (INFOCOM), 2008, pp. 2297-2305.

[13]. S. Antonatos, M. Locasto, S. Sidiroglou, A. D. Keromytis, and E. Markatos. Defending against next generation through network/endpoint collaboration and interaction. In Proc. of the IEEE Int. Conf. on ComputerNetwork Defense, LNCS, vol. 30, 2008, pp. 131-141.

[14]. R. Smith, C. Estan, and S. Jha. Backtracking Algorithmic Complexity Attacks Against a NIDS. In Proc. of the Annual Computer SecurityApplications Conference, Dec. 2006, pp. 89-98.

[15]. C. Castelluccia, E. Mykletun, and G. Tsudik. Improving Secure Server Performance by Re-balancing SSL/TLS Handshakes. In Proc. of the ACMSymposium on Information, Apr. 2005, pp. 26-34.