International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 4 Issue: 3 25-Apr-2015,ISSN_NO: 2321-3337

Prevention Of Surreptitious Denial Of Service in Cloud Computing

[1]M.Astalakshmi , [2]K.Shilpa , [3]Mrs.P.Vijayalakshmi , [4]Mrs.V.Anitha Moses
[1,2]PG Scholar , [3,4]Assistant Professor,
Department of MCA, Panimalar Engineering College

Abstract—*The success of the Cloud Computing paradigm is due to its agreed-application, environment-treaty, and wage-in-usagelandscape. Rendering to this example, the properties of Denial of Service (DoS) attacks involve not only the quality of the carriedpackage, nonethelesslikewise the facilitykeepprices in terms of reserveingestion. Specifically, the lengthier the findingstay is, the complex the charges to be suffered. Consequently, aexactkindness has to be paid for quietDoSoccurrences. They purpose at diminishing their prominence, and at the similarstretch, they can be as harmful as the brute-force attacks. They are urbaneoccurrences personalized to power the worst-case performance of the target systemthrough specific periodic, pulsing, and low-rate circulationshapes. In this paper, we suggest a plan to orchestrate silentspelldecorations, which exhibit a slowly-increasing-intensity trend designed to inflict the maximum financial cost to the fogbuyer, whereasregarding the occupationextent and the provision arrival rate imposed by the detection mechanisms. We describe both how to apply the plannedplan, and*

Keywords—RaincloudComputing, erudite attacks strategy, stumpy-rate attacks, interference detection.

1.INTRODUCTION

Cloud Computing is an emerging paradigm that allows customers to obtain cloud resources and services according to an on-demand, self-service, and pay-by-use business model. Service Level Agreements (SLA) regulate the costs that the cloud customers have to pay for the provided Quality of Service (QoS) [1]. A side effect of such a model is that, it is prone to DoS and Distributed DoS (DDoS), which aim at reducing the service availability and performance by exhausting the resources of the service's host system (including memory, processing resources, and network bandwidth) [2]. Such attacks have special effects in the cloud due to the adopted pay-by-use business model.

Specifically, in Cloud Computing also a partial service degradation due to an attack has direct effect on the service costs, and not only on the performance and availability perceived by the customer. The delay of the cloud service provider to diagnose the causes of the service degradation (*i.e.*, if it is due to either an attack or an overload) can be considered as a security vulnerability. It can be 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, which went down for 19h [3]. Therefore, the cloud management system has toimplement specific countermeasures in order to avoid paying credits in case of accidental or deliberate intrusion that cause violations of QoS guarantees.

Over the past decade, many efforts have been devoted to the detection of DDoS attacks in distributed systems.

Security prevention mechanisms usually use approaches based on ratecontrolling, time-window, worst-case threshold, and patternmatching methods to discriminate between the nominal system

operation and malicious behaviors [4]. On the other hand, the attackers are aware of the presence of such protection mechanisms. They attempt to perform their activities in a “stealthy” fashion in order to elude the security mechanisms, by orchestrating and timing attack patterns that leverage specific weaknesses of target systems [5]. They are carried out by directing flows of legitimate service requests against a specific system at such a low-rate that would evade the DDoS detection mechanisms, and prolong the attack latency, *i.e.*, the amount of time that the ongoing attack to the system has been undetected.

We show that the features offered by the cloud provider, to ensure the SLA negotiated with the customer (including the load balancing and auto-scaling mechanisms), can be maliciously exploited

by the proposed stealthy attack, which slowly exhausts the resources provided by the cloud provider, and increases the costs incurred by the customer.

2. BACKGROUND AND RELATED WORK

Sophisticated DDoSattaks are defined as that category of attacks, which are tailored to hurt a specific weak point in the target system design, in order to conduct denial of service or just to significantly degrade the performance [12], [7]. The term stealthy has been used in [13] to identify sophisticated attacks that are specifically designed to keep the malicious behaviors virtually invisible to the detection mechanisms.

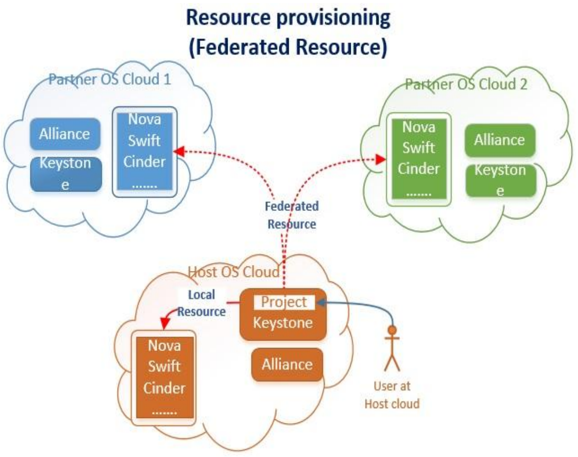
The methods of launching sophisticated attacks can be categorized into two classes: job-content-based and jobs arrivalpattern-based. The former have been designed in order to achieve the worst-case complexity of O(n) elementary operations per submitted job, instead of the average case complexity of O(1) [14], [15], [16]. The jobs arrival patternbased attacks exploit the worst case traffic arrival pattern ofrequests that can be applied to the target system [7], [17]. In general, such sophisticated attacks are performed by sending a low-rate traffic in order to be unnoticed by the DDoS detection mechanisms.

Due to its high similarity to legitimate network traffic and much lower launching overhead than classic DDoSattack, this new assault type cannot be efficiently detected or prevented by existing network-based solutions [21], [22]. Therefore, in recent years, the target of DDoS attacks has shifted from network to application server resources and procedures. The attack takes advantage of the capacity to forecast the time at which the responses to incoming requests for a given service occur. This capability is used to schedule an intelligent pattern in such a way that the attacked server becomes busy the most

time in processing of the malicious requests instead of those from legitimate users.

2.1 Cloud Resources Provisioning

Cloud providers offer services to rent computation and storage capacity, in a way as transparent as possible, giving the impression of ‘unlimited resource availability’. However, such resources are not free. Therefore, cloud providers allow customers to obtain and configure suitably the system capacity, as well as to quickly renegotiate such capacity as their requirements change, in order that the customerscanpay only for resources that they actually use. Several cloud providers offer the ‘load balancing’ service for automatically distributing the incoming application service requests across multiple instances, as well as the ‘auto scaling’ service for enabling consumers to closely follow the demand curve for their applications (reducing the need to acquire cloud resources in advance). In order to minimize the customer costs, the auto scaling ensures that the number of the application instances increases seamlessly during the demand spikes (to maintain the contracted performance), and decreases automatically during the demand lulls.

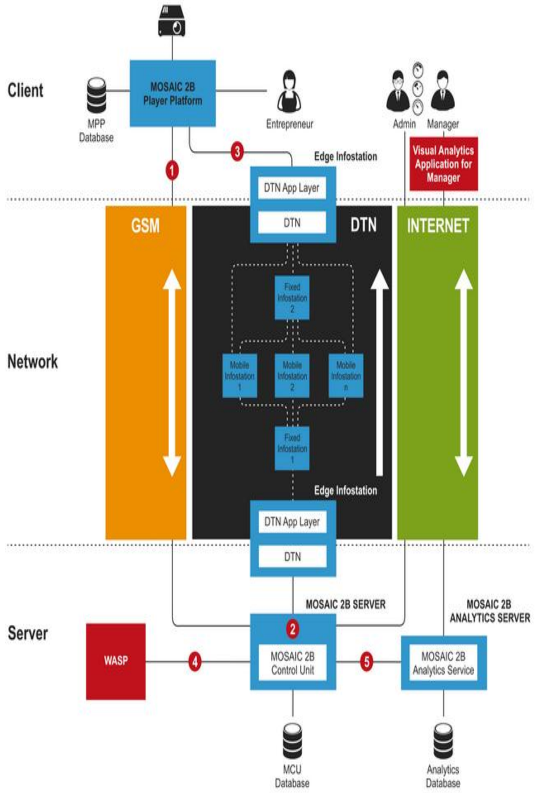


2.2 Related Work

Sophisticated DDoSattaks are defined as that category of attacks, which are tailored to hurt a specific weak point in the target system design, in order to conduct denial of service or just to significantly degrade the performance [12], [7]. The term stealthy has been used in [13] to identify sophisticatedattacks that are specifically designed to keep the malicious behaviors virtually invisible to the detection mechanisms. These attacks can be significantly harder to detect compared with more traditional brute-force and flooding style attacks [5]. The jobs arrival pattern based attacks exploit the worst case traffic arrival pattern of requests that can be applied to the target system [7], [17]. Ingeneral, such sophisticated attacks are performed by sending a low-rate traffic in order to be unnoticed by the DDoS detection mechanisms. In recent years, variants of DoS attacks that use low-rate traffic have been proposed when the Platform detects that a Cloudlet is overloaded (*e.g.*, it has too messages onthe intercommunicating queues), it may choose to start a new Cloudlet instance. The Platform assumes such a decision on the base of policies defined by the application developer (through specific mOSAIC features). Finally, a load balancing mechanism automatically balances the application service.

2.2 The MOSAIC Framework

The MOSAIC project aimed at offering a simple way to develop and manage applications in a multi-cloud environment [11]. It provides a framework composed of two main components: the Cloud Agency and the Software Platform. The Cloud Agency acts as a provisioning system, brokering resources from a federation of cloud providers. The MOSAIC user develops the application on its local machine, then it uses a local instance of the Cloud Agency in order to start-up the process of remote resource acquisition and to deploy the Software Platform and the developed application. The Platform enables the execution of the developed applications on the acquired cloud resources. The Platform assumes such a decision on the base of policies defined by the application developer (through specific mOSAIC features). Finally, a load balancing mechanism automatically balances the application service.



The Platform assumes such a decision on the base of policies defined by the application developer(through specific MOSAIC features). Finally, a load balancing mechanism automatically balances the application service requests among the instances.The Platform assumes such a decisionon the base of policies defined by the application developer (through specific mOSAIC features). Finally, a load balancing mechanism automatically balances the application service requests among the instances. A MOSAIC application is a collection of Cloudlets, which are interconnected through communication resources, such as queues or shared key-value stores. The Cloudlets run on a dedicated operating system, named mOS (mOSAIC Operating System), which is a small Linux distribution. At run-time, the Software Platform transparently scales the Cloudlets instances on the acquired virtual machines (VM) on the base of the resource consumption(auto scaling).

3. DOS ATTACKS AGAINST CLOUD APPLICATIONS

In particular, we consider DDOS attacks that exploit application vulnerabilities [10], [30], [12], including: the Oversize Payload attack that exploits the high memory consumption of XML processing; the Oversized Cryptography that exploits the flexible usability of the security elements defined by the WS-Security specification (*e.g.*, an oversized security header of a SOAP message can cause the same effects of an Oversize Payload, as well as a chained encrypted key can lend to high memory and CPU consumptions); the Resource Exhaustion attacks use flows of messages that are correct regarding their message structure, but that are not properly correlated to any existing process instance on the target server (*i.e.*, messages that can bediscarded by the system, but at the expense of a huge amount
of redundant work,

3.1 FURTIVE DOS DESCRIPTION AND MODELING

This section defines the characteristics that a DDoS attack against an application server running in the cloud should have to be stealth. quality of service provided to the user, we assume that the system performance under a DDoS attack is more degraded, as higher the average time to process the user service requests

3.2 Server Under Attack Model

In order to assess the service degradation attributed to the attack, we define a synthetic representation of the system under attack. We suppose that the system consists of a pool of distributed VMs provided by the cloud provider, on which the application instances run.

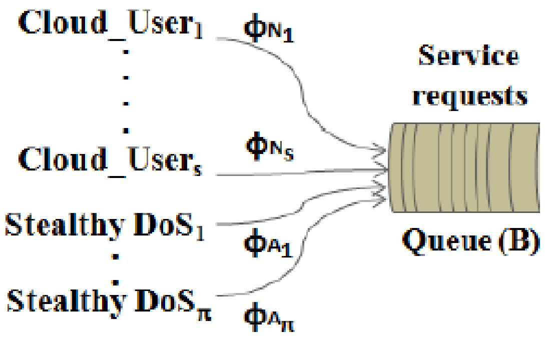


Fig. 1. Attack scenario

4. CONCLUSIONS

In this paper, we propose a strategy to implement stealthy attack patterns, which exhibit a slowly-increasing polymorphic behavior that can evade, or however, greatly delay the techniques proposed in the literature to detect low-rate attacks. Exploiting a vulnerability of the target application, a patient and intelligent attacker can orchestrate sophisticated flows of messages, indistinguishable from legitimate service requests. In particular, the proposed attack pattern, instead of aiming at making the service unavailable, it aims at exploiting the cloud flexibility, forcing the services to scale up and consume more resources than needed, affecting the cloud customer more on financial aspects than on the service availability.

ACKNOWLEDGMENT

This research is partially supported by the European Community’s Seventh Framework Programme (FP7/2007-2013) under Grant Agreements no. 610795 (SPECS), and the MIUR under Project PON02 00485 3487784 “DISPLAY” of the public private laboratory “COSMIC” (PON02 00669).

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/amazon 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.