Available online at http://www.journalijdr.com

IJDR

International Journal of
DEVELOPMENT RESEARCH

ISSN: 2230-9926

International Journal of Development Research
Vol. 6, Issue, 04, pp. 7392-7396, April, 2016

Full Length Research Article

MALICIOUS SOFTWARE PERCEPTION IN CLOUD COMPUTING ENVIRONMENT

Praveen Chandar, J., Rudhra, A., *Yashvanthi, A. and Ragavi, R.

Velammal Institute of Technology, Chennai-600012, India

ARTICLE INFO

Article History:

Received 14th January, 2016
Received in revised form
28th February, 2016
Accepted 21st March, 2016
Published online 27th April, 2016

Key Words:

Cloud computing,
Security,
Kelihos,
DDoS.

ABSTRACT

The usage of cloud computing environment is increasingly common and we rely on it for various services. Cloud services means services made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers. Cloud services are designed to provide easy, scalable access to applications, resources and services, and are fully managed by a cloud services provider. A cloud service can dynamically scale to meet the needs of its users, and because the service provider supplies the hardware and software necessary for the service, there's no need for a company to provision or deploy its own resources or allocate IT staff to manage the service. A cloud usually possesses profound resources, and has full control and dynamic allocation capability of its resources. Therefore, cloud offers us the potential to overcome DDoS attacks. However, individual cloud hosted servers are still vulnerable to DDoS attacks if they still run in the traditional way. Distributed denial-of-service (DDoS) attacks pose a serious threat to network security. There have been a lot of methodologies and tools devised to detect DDoS attacks and reduce the damage they cause. Still, most of the methods cannot simultaneously achieve. The Paper shows an approach to the detection of the various malware and DDoS attack.

INTRODUCTION

A cloud usually possesses profound resources. Data sharing is a vital practicality in cloud storage. These need to be secure inorder to face challenges such as DDoS (Distributed denial-of service) attacks, delay in response from cloud server. The approach taken in this paper relies on the principles and guidelines provided by an existing resilience framework (Michael R. Watson, 2015). The cloud offers us the potential to overcome DDoS attacks. But individual cloud hosted servers are still vulnerable to DDoS attacks if they still run in the traditional way. Stealthy attack as one that is remains undetected by the client computer. A strategy to orchestrate stealthy attack patterns, which exhibit a slowly-increasing-intensity trend designed to inflict the maximum financial cost to the cloud customer, while respecting the job size and the service arrival rate imposed by the detection mechanisms. At the infrastructure level we consider: the elements that make up a cloud datacenter, i.e. cloud nodes, which are hardware servers that run a hypervisor in order to host a number of Virtual Machines (VMs); and network infrastructure elements that provide the connectivity within the cloud and connectivity to external service users. A cloud service is provided through one or more interconnected VMs that offer access to the outside world (Michael R. Watson, 2015). IaaS clouds present the most challenges in terms of maintaining a properly functioning system. Such a system would ideally be free from malware and from vulnerabilities that could lead to an attack. It is for this reason that we focus on this type of cloud since security measures applicable to IaaS clouds. In Existing system, the cloud can detect only the frequent requests from the same ip address and it uses SVM (Support Vector Machine) algorithm to detect the attack and it fails to detect the frequent requests from the multiple system. The proposed system overcomes this disadvantage that is the cloud server can able to detect the frequent requests from the multiple system and block the system by using time based detection and heap space monitoring algorithm.

Corresponding author: Yashvanthi, A.
Velammal Institute of Technology, Chennai-600012, India

Related Works

Malware Analysis

The deployment of cloud computing environments is increasingly common, and we are implicitly reliant on them for many services. However, their dependence on virtualized computer and network infrastructures introduces risks related to system resilience. In particular, the virtualized nature of the

cloud has not yet been thoroughly studied with respect to security issues including vulnerabilities and appropriate anomaly detection. This paper proposes an approach for the investigation and analysis of malware in virtualized environments. We carry out an analysis, on a system and network-wide scale, and further pinpoint some system and network features specifically by studying the example of the Kelihos malware (Safaa Salam Hatem, 2014). The Kelihos malware was first detected in 2010 and has since been developed into new variants that perform a range of attacks such as phishing and spamming (Michael R. Watson, 2015).

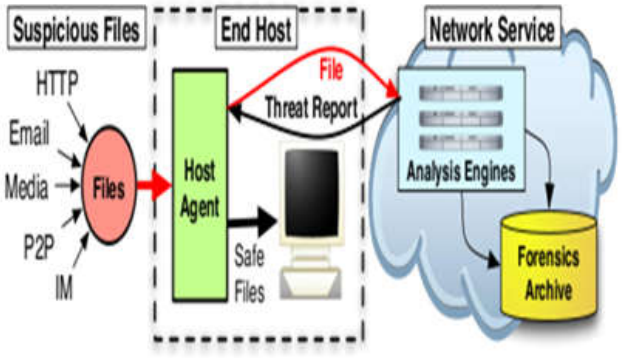

Fig. 1. The Flow of the Process of the cloud computing systems

Anamoly Detection

The online detection of anomalies is a vital element of operations in data centers and in utility clouds like Amazon EC2. Given ever-increasing data center sizes coupled with the complexities of systems software, applications, and workload patterns, such anomaly detection must operate automatically, at runtime, and without the need for prior knowledge about normal or anomalous behaviors. Further, detection should function for different levels of abstraction like hardware and software, and for the multiple metrics used in cloud computing systems. This paper proposes EbAT – Entropy-based Anomaly Testing – offering novel methods that detect anomalies by analyzing for arbitrary metrics their distributions rather than individual metric thresholds. Entropy is used as a measurement that captures the degree of dispersal or concentration of such distributions, aggregating raw metric data across the cloud stack to form entropy time series. For scalability, such time series can then be combined hierarchically and across multiple cloud subsystems. Experimental results on utility cloud scenarios demonstrate the viability of the approach. EbAT outperforms threshold-based methods with on average 57.4% improvement in accuracy of anomaly detection and also does better by 59.3% on average in false alarm rate with a 'near-optimum' threshold-based method (Kaufman, 2009).

Intrusion Detection

Cloud Computing is a general concept of the computing service which is reliance on the Internet for satisfying the computing needs of the users. The providers and the users of the service will be benefit for the new organization pattern. In this paper, we propose a framework for the construction of a CP intrusion detection system in E-Government. The idea can help people construct a flexible security system based on a well-organized strategy and statistical model (Shirazi, 2014).

Virtual Introspection

In (Safaa Salam Hatem, 2014; Marnerides, 2015 and Kaufman, 2009) the specific security threats and challengesintroduced into clouds through the use of core virtualizationtechnologies are discussed. Despite the end-user benefitsgained by virtualization it also comes with a range ofthreats that include: exploits to security holes on virtualmachines (e.g. rootkit attacks on virtual machines (Shirazi, 2014)); mutated cloud-specific Internet-based attacks that aim to compromise cloud networks (e.g. malware (Shirazi, 2014 and Safaa Salam Hatem, 2014) and DDoS attacks on cloud services (Shirazi, 2014 and Michael R. Watson, 2015)). While static examination of computer systems is an important part of many digital forensics investigations, there are often important system properties present only in volatile memory that cannot be effectively recovered using static analysis techniques, such as offline hard disk acquisition and analysis. An alternative approach, involving the live analysis of target systems to uncover this volatile data, presents significant risks and challenges to forensic investigators as observation techniques are generally intrusive and can affect the system being observed. This paper provides a discussion of live digital forensics analysis through virtual introspection and presents a suite of virtual introspection tools developed for Xen (VIX tools). The VIX tools suite can be used for unobtrusive digital forensic examination of volatile system data in virtual machines, and addresses a key research area identified in the virtualization in digital forensics research agenda (Marnerides, 2015).

Multilevel Dependencies

Localizing the sources of performance problems in large enterprise networks is extremely challenging. Dependencies are numerous, complex and inherently multi-level, spanning hardware and software components across the network and the computing infrastructure. To exploit these dependencies for fast, accurate problem localization, we introduce an Inference Graph model, which is well adapted to user-perceptible problems rooted in conditions giving rise to both partial service degradation and hard faults. Further, we introduce the Sherlock system to discover Inference Graphs in the operational enterprise, infer critical attributes, and then leverage the result to automatically detect and localize problems. To illuminate strengths and limitations of the approach, we provide results from a prototype deployment in a large enterprise network, as well as from tested emulations and simulations. In particular, we find that taking into account multi-level structure leads to a 30% improvement in fault localization, as compared to two-level approaches (Safaa Salam Hatem, 2014).

Proposed Method

OpenStack provides infrastructure as a service that let users deploy virtual machines and other instances which handle different tasks for managing a cloud environment. Proposed system is ideally free from malware and from vulnerabilities

since security measures are applied to IaaS Open Stack clouds. In a proposed system, the strategy called SIPDAS (Slowly Increasing polymorphic DDoS Attack Strategy) to orchestrate stealthy attack patterns against applications running in the cloud. Stealthy DDoS Detection mechanism, the server maintains the records of the request given by the user. If the Server loads increases it checks the each individual request of an user, if the request given by the user exceeds the server limit, that particular user IP address is blocked, and the service is denied to that user.

Openstack Configuration and Cloud Services

The Openstack provides a platform for cloud based services. Inorder to provide the Openstack configuration the following setting is done: Router IP address and WLAN settings. After Router setup, Virtual Box is installed. Disk space will be allocated to Virtual Box. Virtual appliance is imported in Virtual Box.

Fig. 2. Open Stack

The cloud server provides the services like video, image and software. The cloud service provider enables the user to upload and download above services. The video service is used to provide the video which is visible to all that we can also download and play the video. The image service used to view the image. The software service is used to download the available software in the server.

Botmaster Application

In this proposed system, creating an application for Botmaster where botmaster has the access for login and will view the description of a type of detection mechanism maintained on the cloud server. This application will intimate the botmaster about the Cloud Virtual instances. The botmaster is configured to perform stealthy denial of service attack to the cloud virtual instances by injecting malware in each Vms.

SIPDAS

SIPDAS (Slowly Increasing polymorphic DDoS Attack Strategy) can be applied to several kind of attacks that leverage known application vulnerabilities, in order to degrade the service provided by the target application server running in the cloud. The term polymorphic is inspired to polymorphic attacks which change message sequence at every successive infection in order to evade signature detection mechanisms. Using SIPDAS, Botmasters perform attack into cloud through bots. Bots create URL, to call cloud for slow their process. If this process continues, cloud performance is slow and it does not response any other client's request. If n number of request in a shorter duration of time from a single IP will be considered as a DoS (Denial of service) Attack. These kinds of attack will be deducted by the cloud instances. We implements SIPDAS a Stealthy Distributed Denial of Service Strategy DDoS in which gradual flooding of request from various Bots is send through BotMaster. These kinds of attack implementation is hard to detect by the Cloud virtual instances.

DDOS and malware detection in open stack cloud

In an existing approach, the DDoS detection mechanism is used to identify number of request given by the user in a particular IP address. The attacker is used to attack the server by using the genuine user IP address and attacker gives the large number of request to that server with a same IP address. The DDoS detect that attack by monitoring the largest number of request is given by the same IP address in a certain time is considered to be a DDoS attack and that particular IP is blocked by the server. In our proposed system, we use a stealthy DDoS Detection mechanism, the server maintains the records of the request given by the user. The server monitors for the memory usage of request in a particular period of time and efficiently able to detect the such kind of attacks. If the Server loads increases in a proactive manner the IPs will be monitored continuously. Those IPs will be block listed. Now the cloud virtual instances removes all the unused memories allocated to the blocked IP request So as to resume to the normal state.

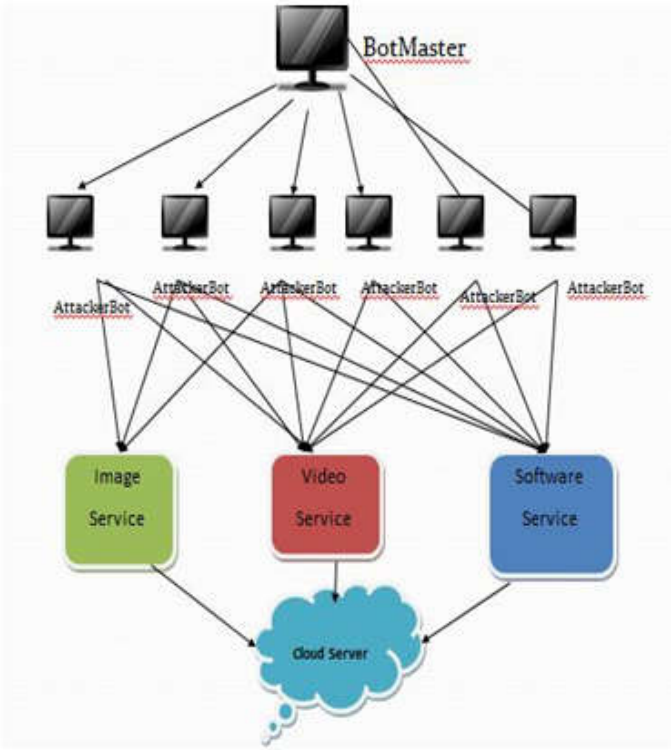

Fig. 3. Architecture Diagram

Algorithms

In our project we used two mechanisms that detect malware attack in cloud especially Iaas cloud namely *Time based mechanisms* and *Heap space Monitoring*. This mechanisms will detect the malware that is harming the cloud.

- ***Time based detection***

This mechanisms will detect the malware in cloud by checking the number of requests from the user for a particular time 'n'.For 'n' time internal, a cloud can acquire 'm'requests from the user say some threshold value has been fixed. The cloud server records the ip address of the client user and the number of requests from the user for a particular time. If the requests for a server from the ip address exceeds the threshold value, then the cloud will detect it as malware and try to block the particular ip address, so that the sever performance will be stable. In existing system, the cloud can detect only the numerous requests from a single ip address, so that it blocks. But in our proposed system, the cloud can be able to detect the requests creating malware from multiple ip address. After detecting the ip address the cloud server will block the ip address, to safeguard its system performance and to maintain its normal state of execution

Algorithm*time based detection*(r,T)
Get the req from user
Set a threshold value based on *req* per time
If req > threshold then
Block the ip
end

- ***Heap space Monitoring***

It enables the cloud server to prevent from malware causing attacks. It allocates memory for each ip address. If the allocated memory address for a particular ip exceeds, the server will block the ip address, so that the blocked ip address cannot end anymore requests until it is resumed to the normal state. After blocking the ip address, the server waits for some time and start to use the unused memories. so that the server and its performance remains in a normal state.

Experimental Result

The cloud services are prominent now-a-days and its level of security goes down that results in a financial threat to the cloud users. The experiments we present in this section test the detection of malware in the cloud infrastructures. The DDoS attack pose a serious threat to the Iaas cloud environment. In our proposed system, we detect the DDoS attack and prevent it to make the system reliable. We detect the attack based on time and space i.e for particular time a client are allowed to send some requests that satisfies the threshold value. Whereas in heap space monitoring, the requests are allocated with some memory in the server, if there are frequent requests from some ip address, the server block ip address for some time,to work in a normal condition, and after sometimes, it resumes the ip address from blocked state to normal state. The experiments focus on DDoS attack that makes a system vulnerable by means of some malicious effect.

Conclusion

Thus the IaaS OpenStack Cloud is free from malware and vulnerabilities. DoS attack gets detected using time based detection mechanism and stealthy DDoS attack gets detected using HeapSpace monitoring. Thus the Stealthy DDoS is identified before service denial and the system is resumed to normal state.

REFERENCES

Angelos, K. Marnerides, C. James, A. Schaeffer, S. Sait, A. Mauthe, and H. Murthy, 2013. "Malware Analysis in Cloud Computing: Network and System Characteristics" in Globecom Workshops (GC Wkshps), IEEE.

Bailey, M. Oberheide, J. Andersen, J. Mao, Z. Jahanian, F. and Nazario, J. 2007. "Automated classification and analysis of internet malware," in Recent Advances in Intrusion Detection, ser. Lecture Notes in Computer Science, C. Kruegel, R. Lippmann, and A. Clark, Eds. Springer Berlin Heidelberg, vol.4637, pp. 178–197. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-74320-0 10

Binsalleeh, H., T. Ormerod, A. Boukhtouta, P. Sinha, A. Youssef, M. Debbabi, and L. Wang, 2010. "On the analysis of the zeus botnet crimeware toolkit," in Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on, Aug, pp. 31–38.

Brian Hay, Kara Nance 2008. "Forensics Examination of Volatile System Data Using Virtual Introspection" in ACS SIGOPS Operating System Review Volume 42 Issue 3,April 2008 [Online]. Available: http://doi.acm.org/10.1145/ 1368506.1368517

Chen, Y., Paxson, V. and R. H. Katz, 2010. "Whats new about cloud computing security?" EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2010-5, Jan [Online].Available:http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

Chengwei Wang, Vanish Talwar, Karsten Schwan, Parthasarathy Ranganathan, 2010. "Online Detection of Utility Cloud Anomalies Using Metric Distributions" in Network Operations and Management Symposium (NOMS), IEEE.

Christodorescu, M., Sailer, R., Schales, D. L., Sgandurra, D. and D. Zamboni, 2009. "Cloud security is not (just) virtualization security: A short paper," in Proceedings of the 2009 ACM Workshop on Cloud Computing Security, ser. CCSW '09. NewYork, NY, USA: ACM, 2009, pp. 97–102. [Online]. Available: http://doi.acm.org/10.1145/ 1655008.1655022

Gruschka, N. and Jensen, M. 2010. "Attack surfaces: A taxonomy for attacks on cloud services," in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, July 2010, pp. 276–279.

Gu, G., Porras, P., Yegneswaran, V. Fong, M. and Lee, W. 2007. "Bothunter: Detecting malware infection through ids-driven dialog correlation," in Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, ser. SS'07.Berkeley, CA, USA: USENIX Association, pp. 12:1–12:16. [Online]. Available: http://dl.acm.org/ citation.cfm?id=1362903.1362915

Ibrahim, A., Hamlyn-Harris, J., Grundy, J. and Almorsy, M. 2011. "Cloudsec: A security monitoring appliance for virtual machines in the iaas cloud model," in Network and System Security (NSS), 20115th International Conference on, Sept, pp. 113–120.

Kaufman, L. 2009. "Data security in the world of cloud computing," Security Privacy, IEEE, vol. 7, no. 4, pp. 61–64, July.

Marnerides, A.K., P. Spachos, P. Chatzimisios, and A. Mauthe, 2015. "Malware detection in the cloud under ensemble empirical model decomposition," in Proceedings of the 6th IEEE International Conference on Networking and Computing.

Mazzariello, C., Bifulco, R. and Canonico, R. 2010. "Integrating a network ids into an open source cloud computing environment," in Information Assurance and Security (IAS), 2010 Sixth International Conference on, Aug, pp. 265–270.

Michael R. Watson, Noor-ul-hassan Shirazi, Angelos K. Marnerides, Andreas Mauthe and David Hutchison, 2015. "Malware Detection in Cloud Computing Infrastructures" in IEEE Transactions on Dependable and Secure Computing.

Paramvir Bah, David A. Maltz, Ranveer Chandra, Albert Greenberg, Srikanth Kandula, Ming Zang "Towards Highly Reliable Enterprise Network Services via Inference of Multi-level Dependencies"in SIGCOMM '07 Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications.

Roschke, S. Cheng, F. and Meinel, C. 2009. "Intrusion detection in thecloud," in Dependable, Autonomic and Secure Computing, 2009.DASC '09. Eighth IEEE International Conference on, Dec, pp.729–734.

Safaa Salam Hatem Dr. Maged H. wafy Dr. Mahmoud M. El-Khouly, 2014. "Malware Detection in Cloud Computing"in *International Journal of Advanced Computer Science and Applications*(IJACSA), Vol. 5, No. 4.

Shirazi, N.-U.-H., Simpson, S., Marnerid, A., M. Watson, A. Mau-the, and D. Hutchison, 2014. "Assessing the impact of intra-cloud live migration on anomaly detection," in Cloud Networking(CloudNet), 2014 IEEE 3rd International Conference on, Oct 2014,pp. 52–57.

Wang, C., Viswanathan, K., Choudur, L., Talwar, V. Satterfield, W. and Schwan, K. 2011. "Statistical techniques for online anomaly detection in data centers," in Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on. IEEE, 2011, pp.385–392.

Yizhang Guan, Jianghong Bao, 2009. "A CP Intrusion Detection Strategy on Cloud Computing"in Proceedings of the *International Symposium on Web Information Systems and Applications* (WISA'09) Nanchang, P. R. China, May 22-24, 2009, pp. 084-087.

****