IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-2, Issue-12 E-ISSN: 2347-2693

Survey on Secure Intrusion Detection and Countermeasures in Cloud

Ankitha.M.M[1*] and M. Azath[2]

[1*]*PG Scholar, Met's School of engineering, Calicut university, Kerala, India*
[2]*Head of Department, Department of computer Science, Calicut University*
ankithamadhav@gmail.com, mailmeazath@gmail.com

www.ijcaonline.org

Received: Nov /22 /2014 Revised: Nov/30/2014 Accepted: Dec/12/2014 Published: Dec/31/ 2014

Abstract— Cloud computing refers to both the application delivers services over the internet and the hardware and system software in the data centers that provide those services. Cloud is attracted by many users because of its security and storage features. The main attack faced by cloud is Distributed Denial of Services (DDOS), in which multiple hosts attack made simultaneously in all network. Security is an important issue in the cloud computing, but the problem is how effectively mitigating intruders and chooses correct counter measures. To counterattack insecure attacks from the virtual machines installed in the cloud proposing vulnerability detection, measurement, along with countermeasure mechanism known as NICE(Network Intrusion detection and Countermeasure Evaluation). In this survey aims to analyze intrusion detection and effective countermeasure mechanisms for achieving security on the virtual machines installed in cloud.

Keywords— Cloud Computing, Cloud Security, DDOS Attacks, Intrusion Detection

I. INTRODUCTION

Cloud computing is one of the emerging and revolutionary technology that is going to change the look of the information technology field. Cloud computing is set of resources and services offered through the Internet and these services are delivered from data centers located throughout the world [1]. The data center hardware and software is what collectively call as a cloud. When a cloud is made accessible in a pay-as-you-go way to the general public, call it a public cloud; the service being vended is utility computing. The term private cloud to refer to internal data centers of a business or other organization not formed for the general public. For example the Amazon pricing is high as compared to other and cloud faces the challenge of over provisioning and saturation in these types of cases.

The organization that takes part of cloud must be provide users ample availability of services or products in a presumable, reliable and flexible way [2]. Cloud computing follows a policy of no single point failure is allowed. The main point associated with the companies in the cloud or virtual machines, their sensitive data's contract out must be secured in all way. Cloud computing enable its consumers by providing virtual resources through internet. General example of cloud services is Google apps and Drop Box. Cloud computing aspects mainly deals with the two ideas like storage of various applications and hardware or software resources, and security for the stored data's in the cloud center. In this way cloud provides scalable resources that may be information or applications can be accessed in a low-cost, on demand, flexible way. Many organization, IT industries, companies and users are mitigating towards the cloud features because of its security [3]. Cloud provides security in confidentiality, availability and integrity of stored data's in the data center. The speedy growth in field of "cloud computing" also increases severe security concerns. Lack of security is the only snag in wide adoption of cloud computing. Cloud computing is encircled by many security issues like securing data, securing accessing of data and examining the utilization of cloud by the cloud computing vendors. The exposure in cloud computing has brought lots of security challenges [3]. Among all security problems, abuse and nefarious [4] use of cloud computing is considered as the top security threat. This is the way through the violation of registration and usage; attackers can exploit vulnerabilities in clouds and can utilize cloud system resources to install attacks.

Cloud and its security management have to reassure uninterrupted access to the communication infrastructure. Sometimes cloud is not well protected against attacks from the outside intruders so additional reconnaissance may be necessary. A lot of these cloud data's are also threatened from the inside. Virtually every industry and even some parts of the public sector are taking on cloud computing today, either as a provider or as a consumer. These industries or public sector may use the data's for sharing in between other companies. This data sharing feature can be used for setup intruders by breaking into the web servers. Once weakened these web servers can work as a launching point for conducting further attacks against users in the cloud.

One such major attack is the DoS or its version DDoS attack [5]. Distributed Denial of Service is malicious attacks that make unavailable the resources by temporarily interrupting or suspending services. Particularly, attackers can explore vulnerabilities in a cloud system and compromise virtual machines to deploy further large-scale Distributed Denial-of-Service (DDoS). Cloud users can install vulnerable software on their virtual machines, which essentially contributes to loopholes and security threats in cloud security. Cloud providers nowadays safeguard against DDOS attacks, thefts etc. Virtualization is the foremost security mechanism adopted by today's cloud environment. The cloud computing must be include contract and expect to use laws of security by users rather than other clever techniques. The confront of cloud is that to work well managing traffic, resources, disks, spaces etc even when the number of tasks increases. Cloud computing be in a way of cost-effective manner, but not to violate security level agreements. The problem is to how to establish an effective vulnerability or attack detection and response system for accurately identifying attacks and minimizing the impact of security breach to cloud users.

II. RELATED WORKS

A. Virtualization

The main attack faced by cloud is distributed denial of service (DDoS), in which multiple hosts made simultaneously in all network. For the intrusion detection the proposed system a solution using Dempster-Shafer Theory (DST)[6] operations in 3-valued logic and the Fault-Tree Analysis (FTA)[7]. It uses private cloud using Eucalyptus open source version 2.0.3 as front end and back end as 3 nodes installed on virtual machine as back end [8]. Virtualization is done by xen hypervisor and snort is used for virtual machine based IOS to avoid the overloading problem by the attack. Mysql database is uses to reduce the loss of data and to simplify work of administrator and to increase the usage of virtual machine resources.

B. BotHunter

The leading threat in the cloud malicious threat is s self-propagating application that attack hosts by direct method. Among all the bots, botnet is a collection of slave infected computers with various activities like thefting, DDoS attacking etc. There is a command control (CC) channel which is the communication channel for attacking and through which attacker's updates also. In this approach successful infection is realized by a monitoring system. This approach put forward an evidence trail to check out the bot infection by an infection dialogue correlation strategy, the dialogue correlation categorized or viewed as a loosely unordered data exchange between internal and external entities and these are examined under the actions like target scanning, infection exploit, command and control channel (C&C) establishment, binary egg download, outbound scanning and execution [9, 16]. The alert will recognized with the help of the threshold combination of sequence by watching the evidence sequence with the bot hunters infected dialogue model.

C. BotSniffer

Network and cloud affects many security threat problems, and among those problems botnet can be considered as a main security problem. Botnet is a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam. These botnets have their own characteristics differ from other bots (security threats), so the countermeasure should be different in manner. The command and control channel (CC) of botnet are different from the other bot channels and there is a bot master who take full control over the bot. The main weakest link of botnet is their cc channel and this command and control channel can be taken in to account for the countermeasure and battle against bots by monitoring its network. In this paper proposes a method based on the observation of cc, by making a correlation and a similarity between command and control activities and bots within the same botnets [10, 16]. The system of botsniffer can capture this correlation and use algorithm to detect bots with false positive and false negative rates.

D. SPOT Analysis

The main feature of cloud is having and security. Sometimes this security features and sharing can be used to deploy attack in the cloud through infected virtual machines, called zombies. Cloud may contain vulnerable virtual machines. Identify and mitigating this attacks where a difficult challenge for the cloud administrators. These compromised cloud virtual machines installed work a one of the main key security threat and can dispatch various security attacks like spamming, theft, DDoS deployment etc.

In this paper counteract on the detection of compromised zombies in the spamming environment by an effected mechanism SPOT; by examine outgoing messages of the network. SPOT works based on the method called SPART (Sequential Probability Ratio Test) [11, 16], which worked on two assumptions like outgoing messages are occurred in sequentially and the system like compromised machine and not compromised machine. So by this SPART recognize compromised machine with minimum error rate and SPOT by a threshold value to determine the false positive and negative rate of the system [12, 16].

E. Novel QG Approach

Network intrusion can be multistep and multiple attacks. The defending mechanism against multistep is difficult and challenging task. So it needs to correlate isolated alerts in each individual step in to attack countermeasure by using efficient algorithm. Using infinite memory for alerts in the form of sliding window can make a counter attack, but unfortunately attackers can prevent two attack steps from both falling in to sliding window. Here the new approach called novel queue graph to address this issue, where this queue only keep in memory of latest alert matching each known exploit[13]. This correlation where recorded and the graph approach is used for hypothesizing messaging alerts then predicting future alerts. The correlation will make helpful than just alerting mechanism in intrusion detection system (IDS) [14]. So this method can be said as a programming one.

F. MulVAL

Vulnerability attack detecting, analyzing is a great challenging task for a network administrator, Over these years many vulnerabilities are discovered, detected were recorded for the future work. So to make an effective vulnerability analysis and detection tool, integrated with all formal vulnerability specification from records and spam communities and this must be able to scale to any type of network. Mulval using an end to end multistage and mutihost vulnerability analysis with a data log for the analysis of configuration, description, reasoning rules, bug specification, etc[15]. The inputs to the Mulval analysis are like advisories; for reporting vulnerability, host configuration; about software and services on host, network configuration; how network and firewalls are configured, principles; about the users of network, interaction; components interaction in the model and policy; accessing rights. Mulval make use scanner, OVAL and an analyzer.

Tabe 1: Comparison intrusion detection and countermeasure

Sl no	Method Name	Description	Advantages	Limitation
1	Virtualization	Uses a data fusion methodology in the front-end.	Reduce false negative rate and increase detection rate.	No accuracy in the attack detection from attackers
2	SPOT analysis	SPOT, is based on sequentially scanning outgoing messages while employing SPRT.	Quickly determine whether a host has been compromised or not.	scalability is a big issue
3	BotHunter	Detects compromised machines by correlating the intrusion alarms triggered by inbound traffic.	Scalable and reliable	For any IDS implementation large volume of raw alerts and false alarms are main problems
4	BotSniffer	Detects zombies by grouping flows according to server connections and searching for similar behavior in the flow	detection accuracy with very low false positive rate	Dependent on protocol and network structure
5	Novel queue graph	Detection is by checking latest alerts and correlating them	Monitor the progress of intrusions	Countermeasures are a static method
6	MulVAL	An end to end multistage and mutihost vulnerability anal	Vulnerability analysis can be performed automatically and efficiently	Difficult to correlate alerts

III. CONCLUSION

This survey has focused on the intrusion detection in cloud. The main objective of this paper is to establish an effective vulnerability/attack detection and response system for accurately identifying attacks and reducing the impact of security attacks on cloud. It has been found that each technique has its own benefits and limitations; no technique is best for every case. The main limitation of existing work found to the selection of accurate and good countermeasures for the attacks. Based on the study it recognizes that the graph with good correlation can be used for the effective counter mechanism. Thus proposes a mechanism to prevent vulnerable virtual machines from being compromised in the cloud NICE. It is a multiphase distributed vulnerability discovering, measurement, and selection of counteract mechanism, which is constructed on attack graph based analytical models and reconfigurable virtual network-based countermeasures.

REFERENCES

[1]http://en.wikipedia.org/wiki/Cloud_computing

[2]M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A View of Cloud Computing,” ACM Comm., vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3]H. Takabi, J.B. Joshi, and G. Ahn, “Security and Privacy Challenges in Cloud Computing Environments,” IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, Dec. 2010.

[4]Cloud Security Alliance “Top Threats to Cloud computingv1.0,”https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, Mar. 2010.

[5]B. Joshi, A. Vijayan, and B. Joshi, “Securing Cloud Computing Environment Against DDoS Attacks,” Proc. IEEE Int’l Conf. Computer Comm. and Informatics (ICCCI’12), Jan. 2012.

[6] Dissanayake, A., *Intrusion Detection Using the Dempster-Shafer Theory*. 60-510 Literature Review and Survey, School of Computer Science, University of Windsor, 2008.

[7] Guth, M.A.S., *A Probabilistic Foundation for Vagueness & Imprecision in Fault-Tree Analysis*.IEEE Transactions on Reliability, 40(5), pp.563-569, 1991.

[8]A.M. Lonea, D.E. Popescu, H. Tianfield, Detecting DDoS Attacks in Cloud Computing Environment, INT J COMPUT COMMUN, ISSN 1841-9836, 8(1):70-78, February, 2013.

[9]G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, “BotHunter: Detecting Malware Infection through IDS-driven Dialog Correlation,” Proc. 16th USENIX Security Symp. (SS ’07), pp. 12:1-12:16, Aug. 2007.

[10]G. Gu, J. Zhang, and W. Lee, “BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic,” Proc. 15th Ann. Network and Distributed System Security Symp. (NDSS’08), Feb.2008.

[11] A. Wald. *Sequential Analysis*. John Wiley & Sons, Inc, 1947.

[12] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, “Detecting Spam Zombies by Monitoring Outgoing Messages,” IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198-210, Apr. 2012

[13] B. Morin, L. Me´, H. Debar, M. Ducasse´, M2D2: a formal data model for IDS alert correlation, in: Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection (RAID’02), 2002, pp. 115–137.

[14]L. Wang, A. Liu, and S. Jajodia, “Using Attack Graphs for Correlating, Hypothesizing, and Predicting Intrusion Alerts,” Computer Comm., vol. 29, no. 15, pp. 2917-2933, Sept. 2006.

[15]X. Ou, S. Govindavajhala, and A.W. Appel, “MulVAL: A Logic- Based Network Security Analyzer,” Proc. 14th USENIX Security Symp., pp. 113-128, 2005.

[16]Chun-Jen Jung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee, Dijiang Huang,NICE-Network Intrusion Detection and Countermeasure Selection in Virtual Network System, IEEE Transactions on Dependable and Secure Computing, Issue Vol 10 No 4 2013.

AUTHORS PROFILE

Ankitha.M.M. has completed B Tech in CSE from Jawaharlal College of Engineering and Technology, Palakkad, Kerala, in 2012. Presently she is pursuing her M Tech in CSE from Met’s School of engineering, Thrissur, Kerala. Her research interests include networking, cloud and intrusion detections and security.

Dr. M. Azath is Head of Department of Computer Science and engineering, Met’s School Of Engineering, Mala. He has received Ph.D. in Computer Science and Engineering from Anna University in 2011. He is a member in Editorial board of various international and national journals and also a member of the Computer society of India, Salem. His research interests include Networking, Wireless networks, Mobile Computing and Network Security.