M. Hari Babu *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 7, July- 2015, pg. 8-15 **ISSN: 2321-8363**

DISTRIBUTED INTRUSION DETECTION SYSTEM FOR RESOURCE - CONSTRAINED DEVICES IN NETWORKS

M. Hari Babu
M. Tech (Computer Science)
CSE Dept., JNTUA College of Engineering, Anantapuramu, A.P, India.; harimucheli2@gmail.com

Dr. S. Vasundra
Professor and H.O.D
CSE Dept., JNTUA College of Engineering, Anantapuramu, A.P, India.; vasundaras@rediffmail.com

Abstract

Virtually all sectors and even parts of the public sector take on cloud computing today, either as a supplier or a consumer. Despite being young, he has not been left untouched by hackers, criminals and other "Black hat hackers" from getting into web servers. Once weakened these web servers can provide a point of carrying out new attacks against users in launching cloud. Such an attack is a DoS or DDoS attack version. In particular, attackers can explore the vulnerabilities of a cloud system and jeopardize the virtual machines deployed on a larger scale Distributed Denial-of-Service (DDoS). DDoS attacks commonly involve early career actions such as multi-step operation, low vulnerability scanning frequency, and compromising vulnerable VMs recognized as zombies, and finally DDoS attacks over the zombies compromised. In the cloud system, especially Infrastructure-as-a-Service (IaaS) clouds, detecting zombie probing attacks is extremely difficult. To prevent vulnerable virtual machines to be compromised in the cloud, we propose vulnerability detection spread in phases, measurement, and measurement against-selection mechanism called NICE, which is build on analytical models based graph attack and against measures on the basis of reconfigurable virtual networks. Assessments and security systems demonstrate the effectiveness of the proposed solution.

keywords: Intrusion Detection, Attack Graph, Cloud Computing, Zombie Detection, Network Security.

1. Introduction

Recent studies have revealed that users migrating to cloud security as the most important factor. A Cloud Security Alliance (CSA) recent survey shows that, among all the security issues, abuse and harmful use of cloud computing is considered the high security threat, in which attackers can make use of vulnerabilities in the clouds and use the resources of the cloud system to deploy attack [1]. In conventional data centers, system administrators have complete control over the host machine where vulnerabilities can be detected and corrected by the system administrator in a centralized aspect. However, patching known security holes in cloud data centers, cloud computing where users typically have the privilege to control the software installed on their managed virtual machines may not work effectively and may violate agreement service level (SLA). In addition, cloud users can install the vulnerable software on their virtual machines, which is basically contributes to loop holes in cloud security. The challenge is to create a system vulnerability / attack detection and effective response to accurately identify attacks and minimizing the impact of security violation for users of cloud computing. In, M. Armbrust et al. addressed that the protection of "business continuity and availability of services" service failures is one of the main concerns in cloud computing systems [2]. In a cloud system where the infrastructure is shared by millions of users, abuse and harmful use of shared infrastructure services will make attackers to exploit loop wholes of the cloud and to use its resources to deploy attacks in further efficient ways.

Such attacks are most efficient in the cloud environment considering cloud users usually share computer resources, for example, being connected by the same switch, sharing the same data storage and file systems, even with aggressors potential. The similar configuration for the virtual machines in the cloud, for example, VM OS installed vulnerable software, virtualization techniques, networking, etc., attracts attackers to compromise multiple virtual machines.

2. Literature Survey

Many documents were studied and finally the following were selected for further analysis. The method adopted after the study is briefly outlined at the end of the chapter.
Cloud Computing is the recently emerged technology of distributed computing system. Cloud Computing users focused on API security and afford services to its customers in a multi-tenant environment in three layers namely, software as a service, platform as a service and the infrastructure as a service, with the help of Web services [3]. It offers service facilities to its consumers on request. This service provided can easily invite striker to attack by Saas, PaaS, and IaaS. As resources are gathered at one place in data centers into cloud computing, the DDOS attacks such as HTTP and XML in this environment is dangerous and provides harmful effects and also all consumers will be affected simultaneously. These attacks can be resolved and detected by a proposed methodology. In this method, this problem can be overcome by using the proposed system. Different types of vulnerabilities are detected in the proposed system. The SOAP application allows communication between the client and the service provider. By the help of Service Oriented Trace back architecture the SOAP request is sent to the cloud. In this architecture service oriented is present, which contains within proxy marks incoming packets with source identification message to identify the actual customer. Then, the SOAP message is crossed by X Detector. The X Detectors used to monitors and filter DDoS attacks such as HTTP and XML DDoS attack. Finally the true message of the filtered customer is transferred to the cloud service provider and the corresponding services are delivered to the client securely.

Cloud computing has generated significant interest in both academia and industry, but it is still an open paradigm [4]. Actually, it aims to strengthen the economic utility model with the evolutionary development of many existing approaches and information technologies, including distributed services, applications and information infrastructure including pools of computers, networks and storage resources. There is confusion in the IT community about how a cloud contrasts from existing models and how these changes affect its acceptance. Some may see cloud as a new technical revolution, while others will consider it a native evolution of technology, culture and economy.

1) However, cloud computing is an important paradigm, with the potential to significantly reduce costs through optimization and increased operating and economic efficiency.

2) In addition, cloud computing significantly improve collaboration, agility, and scale, thus enabling a truly global computing model over the Internet infrastructure. However, without suitable security and privacy solutions designed for the cloud computing paradigm revolutionize this potentially could become a huge failure. Many surveys of potential cloud adopters indicate that security and privacy is the main concern obstacle hindering its adoption.

3) This paper illustrates the unique problems of cloud computing that exacerbate the challenges of security and privacy in the clouds.

4) We also discuss various approaches to address these challenges and explore future work required to provide a trusted cloud environment.

In this paper, we focus on the detection of compromised machines in a network are used for mailing spam messages, which are usually referred as mails zombies [5]. Since spamming provides a critical economic incentive for controller's compromise the machines to recruit these machines, it has been widely recognized that many compromised machines are associated in spamming. A number of recent research investigated the characteristics of global aggregates spam botnets (networks of compromised machines involved in spamming), such as the size of botnets and the spamming patterns of botnets [6], based on the sampling of spam messages received in a large email service provider.

3. Proposed Method

We offer NICE (Network Intrusion Detection and Countermeasure selection in virtual network systems) to build a defense-in-depth intrusion detection framework. For better detection of attacks, NICE integrates analytical procedures of attack graphs in the intrusion detection process. We have to note that the design of NICE has no intention of improving one of the existing intrusion detection algorithms; Naturally, NICE uses a reconfigurable approach to virtual networking to detect and defend against attempts to compromise virtual machines, preventing zombie VMs. In general, NICE has two main phases: deploy a thin mirror agent based on an intrusion detection system (NICE-A) on each cloud server to obtain and study the cloud traffic. A NICE-A periodically scans vulnerabilities virtual system within a cloud server to establish Scenario Attack Graph (SAG), and then depending on the severity of the identified vulnerability to attack collaboration objectives, NICE decide or not to put a virtual machine in the inspection State network.

Advantages of proposed work :

- We offer NICE (Network Intrusion Detection and Countermeasures in virtual network systems) to establish a defense-in-depth intrusion detection framework.
- The malicious behavior detection area has been well explored.
- The proposed solution can significantly reduce the cloud system risk from being exploit and abused by internal and external attackers.

Proposed technique :

- Scenario Attack Graph (SAG).

4. Implementation

The implementation shows that the theoretical design has proven in a working system. Hence, it can be studied the most critical step in the implementation of a new system successfully and giving the user confidence that the current system works and is effective. The implementation is a milestone in software development where the software design is implemented as a set of program units. Objects that are identified in the design phase are implemented and functions that manipulate these objects are made. The proposed method was implemented using JDK.

NICE Architecture with one cloud server cluster:

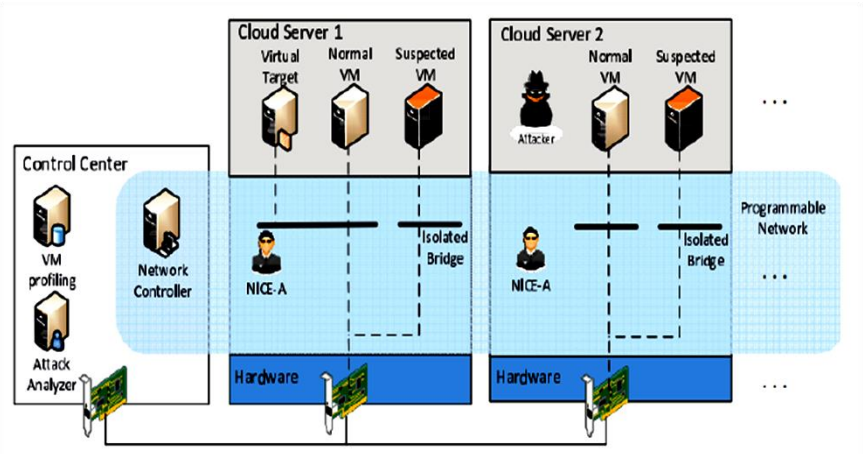

Figure 1: Nice Architecture with one cloud server

The proposed system is designed to operate in a cloud virtual network environment. It consists of a cloud server cluster and their interconnections. We assume that the latest virtualization solutions are deployed on cloud servers. The virtual environment can be classified as Privilege areas, for example, the dom0 of XEN servers [7] and the KVM host domain [8] and non-privileged areas, for example, the virtual machines. Cloud servers are interconnected by programmable network switches, such as the physical Open Flow Switches (OFS) [9] and software-based Open V Switches (OVS) [10] deployed in privileged areas. In this work, we refer OFSs and OVS and controllers for the Software Defined Network (SDN). Expanded security mechanism focuses on providing a non-intrusive approach to prevent attackers from exploring vulnerable VM and use them as a springboard for new attacks.

5. System Components

The various modules used in the system are:
1. Nice-A
2. Countermeasure Selection
3. VM Profiling
4. Attack Analyzer
5. Network Controller

1. Nice-A

The NICE-A is a Network-based Intrusion Detection System (NIDS) agent installed in each cloud server. It analyzes the traffic passing through the bridges which control all traffic between virtual machines and in / out physical cloud servers. It will sniff a mirror port on every virtual bridge in the Open v Switch. Each bridge forms a remote subnet in the virtual network and linked to all the corresponding virtual machines.

The traffic generated from the VMs on the mirrored software bridge will be mirrored to a specific port on a specific bridge using SPAN, RSPAN, or ERSPAN methods. It is more effective to analyze the cloud server traffic of all traffic in the cloud server needs to go through it; but our design is independent to the VM which is installed. The false alarm rate could be reduced through our architecture design.

2. Countermeasure Selection

Countermeasure Selecting to illustrate how NICE works, consider an example, an alert is generated for the node 16 (vAlert = 16) when the system detects buffer overflow. After the alert is generated, the cumulative probability of node 16 is 1 because the attacker has already compromised the node. This triggers a change in cumulative probabilities of leaf nodes of node 16. Now the next step is to select the countermeasures from the pool of countermeasures CM.

3. VM Profiling

The virtual machines in the cloud can be summarized to obtain precise information about their condition, services running, open ports, etc. An important factor that has to VM profile is its connectivity with other virtual machines. It is also the knowledge of services running on a Virtual Machine in order to verify the authenticity of alerts relating to this VM. An attacker can use the port scanning program to perform an intense review of the network looking for open ports on any VM. Hence, information on open ports of a virtual machine and the history of open ports play an important role in determining the vulnerability of the VM. All these factors collective will form the VM profile. VM profiles are stored in a database and contain information about vulnerabilities, alerts and traffic.

4. Attack Analyzer

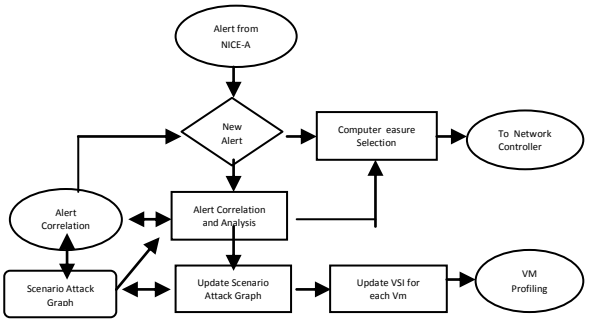

Fig. 2 Flow Chart for Attack Analyzer

The main functions of NICE system are performed by attack analyzer, which includes procedures such as the attack graph construction and update, on the alert correlation and countermeasure selection. The process of building and using the Scenario Attack (SA) consists of three phases: information gathering, attack graph construction, and potential exploit path analysis. With this information, the attack paths can be modeled using SA. Each node in the graph represents an exploit attack by the attacker. Each path from an initial node to a goal node represents a successful attack.

5. Network Controller

The network controller is a key element to support the programmable networking capability to perform the reconfiguration of virtual network. In NICE, we have integrated control functions for both the OFS and OVS in the network controller allows the cloud system to set security /filtering rules in an incorporated and comprehensive manner. The network controller is answerable for the collection of open flow of current network information and provides data to the analyzer of attack to build graphical attack. In NICE, network control also consults with the analyzer of attack to the flow of access control by setting up filtering rules on the corresponding OVS and OFS. The network controller is also responsible for the implementation of the attack against the analyzer. According to VM security index and severity of an alert, the countermeasures are chosen by NICE and executed by the network controller.

6. Performance Analysis

The amount of CPU utilized by MDIDS is less when compared to other intrusion detection system. The graph below highlights this fact.

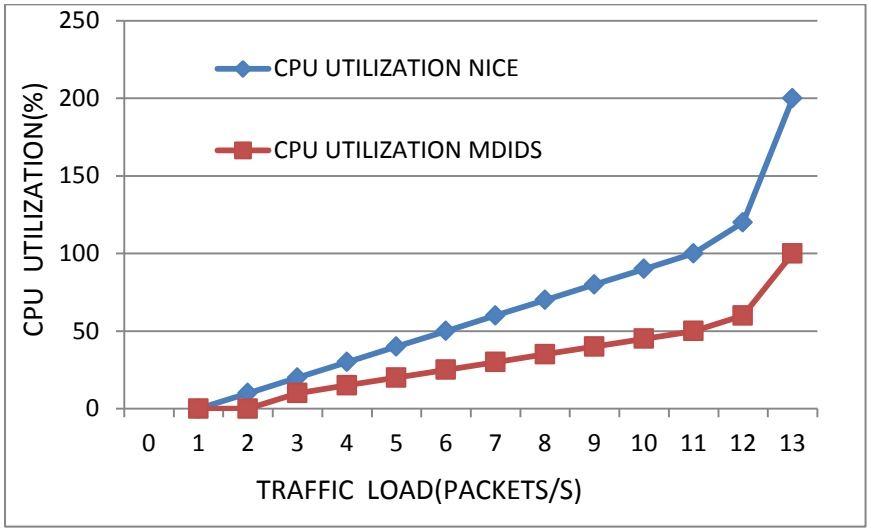

Fig. 3 CPU Utilization in MDIDS

The CPU utilization in mirror based MDIDS [11], proxy based MDIDS and MDIDS are compared. The CPU utilization is very low in MDIDS than in other two intrusion detection system. The CPU utilization is given in percentage against traffic load measured in packets per second. Proxy based MDIDS utilizes twice the amount of CPU than MDIDS for a traffic load of 15 packets per second. Mirror based MDID utilizes 35% more CPU than MDIDS for an equal traffic load. The IRT is analyzed in two phases. The IRT is calculated with the number of applications plotted against its response time measured in milliseconds. In the first phase IRT is calculated without the introduction of MDIDS in cloud.

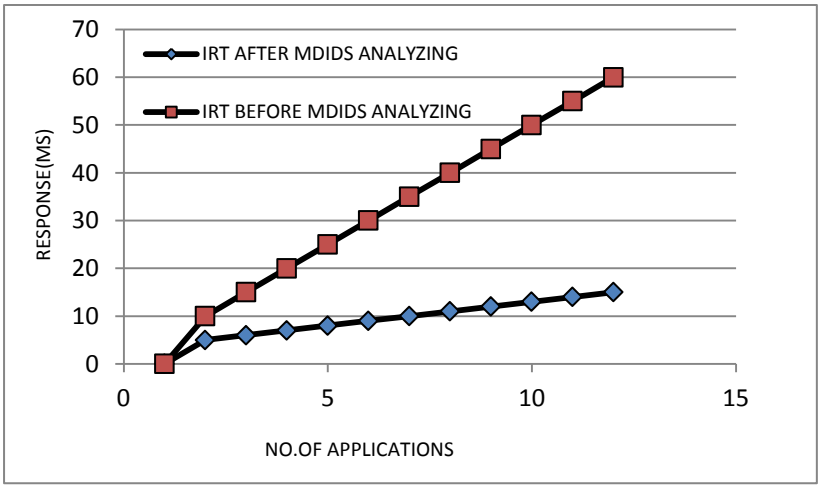

Fig. 4 Infra-structure Response Time Calculation

The IRT is very high before introducing MDIDS. The IRT becomes very low after the introduction of MDIDS. This clearly indicates that there is growth in the performance of cloud in MDIDS. The service to the clients is implemented rapidly in MDIDS. The time taken to create a required VM before detecting DDOS using MDIDS is more.

The time in milliseconds and the number of VM created are noted and plotted. Before analyzing the DDOS , the VM creation taking 100milliseconds after detecting the DDOS using MDIDS the VM creation taking only 10milli-seconds The time taken to create one VM before detection is ten times the time taken to create it after detection.

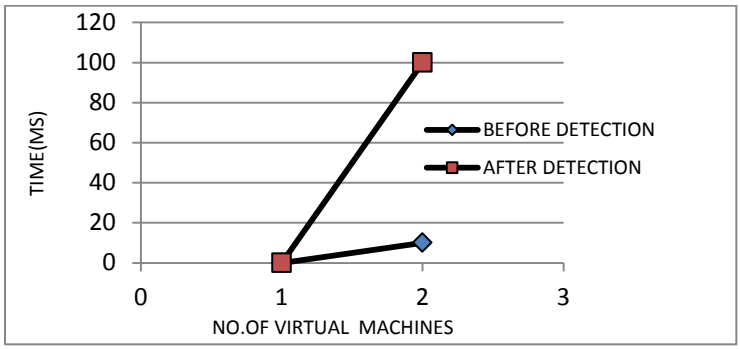

Fig. 5 Time Taken to Create Virtual Machine

7. Conclusion

This paper provides Network Intrusion detection and Countermeasure selection and the related security concepts. NICE, which is expected to detect and mitigate mutual attacks in the cloud virtual networking environment. NICE uses the attack graph model to conduct attack prediction and detection. The proposed solution investigate how to use the programmability of software switches based solutions to advance the detection accuracy and defeat victim exploitation phases of mutual attacks. The system performance evaluation indicates the feasibility of NICE and shows that the proposed solution can considerably reduce the risk of the cloud system from being exploited and misused by internal and external attackers.

References

1) Coud Sercurity Alliance, "Top threats to cloud computingv1.0, "https://cloudsecurityalliance.org/topthreats /csathreats.v1.0.pdf, March 2010.
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 Commun., vol. 53, no. 4, pp. 50–58, Apr. 2010.
3) B. Joshi, A. Vijayan, and B. Joshi, "Securing cloud computing environment against DDoS attacks," IEEE Int'l Conf. Computer Communication and Informatics (ICCCI'12), Jan. 2012.
4) H. Takabi, J. B. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security & Privacy, vol. 8, no. 6, pp. 24–31, Dec.2010.
5) 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. IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTING
6) G. Gu, J. Zhang, and W. Lee, "BotSniffer: detecting botnet command and control channels in network traffic," Proc. of 15th Ann. Network and Distributed Sytem Security Symp. (NDSS '08), Feb. 2008.
7) "Citrix XenServer." [Online]. Available: http://www.citrix.com/xenserver.
8) "Kernel based Virtual Machine (KVM)." [Online]. Available:http://www.linuxkvm.org/
9) "Openflow."http://www.openflow.org/wp/learnmore/, 2012.
10) "Open vSwitch project," http://openvswitch.org, May 2012

11) S.Usha, Dr.A.Tamilarasi, R.Kalaivanan "MDIDS: Multiphase Distributed Intrusion Detection in Virtual Network Systems" IJSET (ISSN : 2277-1581) Volume No.3 Issue No.4,
pp : 355-358

Authors:

Mucheli Hari babu received B.Tech degree in Information Technology from Narayana Engineering College, gudur, A.P Affiliated to JNTU hyderabad, A.P, during 2007 to 2011. Currently pursuing M.Tech in Computer Science from JNTUA College of Engineering, Anantapuramu, A.P, India. Area of interests include Computer Networks, Network Security.

Dr. S. VASUNDRA, presently working as Professor and Head of the Department CSE, JNTUA CEA. She completed her Ph.D from JNTUA university, anantapur, M.Tech from JNTUA and B.E from VTU. She is having 16 years of teaching experience and 5 years of research experience. Published 20 papers in various international journals and 3 in national journals. Her areas of interest include MANET's, Cloud Computing, Algorithms, Data Structures and Distributed Computing.

