Privacy Preserving Against Network Intrusion Detection in Virtual Network System

Shruthi S[1] Mrs. Sudhamani M J[2]
[1]M.Tech-II Year Dept. of Computer Science
[2]Assistant Professor, Dept. of Computer science
[1, 2] RNSIT, Bangalore, India

Abstract— Cloud security is one of most important issues that has attracted a lot of research and development effort in past few years. Particularly, attackers can explore vulnerabilities of a cloud system and compromise virtual machines to deploy further large-scale Distributed Denial-of-Service(DDoS). DDoS attacks usually involve early stage actions such as multi-step exploitation, low frequency vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks through the compromised zombies. Within the cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie exploration attacks is extremely difficult. This is because cloud users may install vulnerable applications on their virtual machines. To prevent vulnerable virtual machines from being compromised in the cloud, we propose a multi-phase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE, which is built on attack graph based analytical models and reconfigurable virtual network-based countermeasures**.**

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

I. INTRODUCTION

A recent Cloud Security Alliance (CSA) survey shows that among all security issues, use of cloud computing is considered as the top security threat, in which attackers can exploit vulnerabilities in clouds and utilize cloud system resources to deploy attacks. In traditional data centers, where system administrators have full control over the host machines, vulnerabilities can be detected and patched by the system administrator in a centralized manner. However, patching known security holes in cloud data centers, where cloud users usually have the privilege to control software installed on their managed VMs, may not work effectively and can violate the service level agreement (SLA). Furthermore, cloud users can install vulnerable software on their VMs, which essentially contributes to loopholes in cloud security. The challenge is to establish an effective vulnerability/attack detection and response system for accurately identifying attacks and minimizing the impact of security breach to cloud users.

In this paper it is mainly used to analyze and detect the attacker. In a cloud system where the infrastructure is shared by potentially millions of users, abuse and infamous use of the shared infrastructure benefits attackers to exploit vulnerabilities of the cloud and use its resource to deploy attacks in more efficient ways [3]. Such attacks are more effective in the cloud environment because cloud users usually share computing resources, e.g., being connected through the same switch, sharing with the same data storage and file systems, even with potential attackers [4]. The similar setup for VMs in the cloud, e.g., virtualization techniques, VM OS, installed vulnerable software, networking, and so on, attracts attackers to compromise multiple VMs. Network Intrusion detection and Countermeasure selection in virtual network systems is to establish a defense-in-depth intrusion detection framework. For better attack detection, it incorporates attack graph analytical procedures into the intrusion detection processes. We must note that the design of NICE does not intend to improve any of the existing intrusion detection algorithms; indeed, NICE employs a reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, thus preventing zombie VMs.

After analyzing and detection of explorer the vulnerabilities can be overcome by recovering the data which is lost while attacking. The attacked virtual machine memory can be recovered by data backup and recovery technique. This is one of basic technique for preserving the data of the cloud server.

II. RELATED WORK

A. Securing Cloud Computing Environment Against DDoS Attacks

It describes the senario that in cloud computing where infrastructure is shared by potentially millions of users, Distributed Denial of Service (DDoS) attacks have the potential to have much greater impact than against single tenanted architectures. The paper[1] tested the efficiency of a cloud trace back model in dealing with DDoS attacks using back propagation neural network and finds that the model is useful in tackling Distributed Denial of Service attacks

B. New Alert Correlation Algorithm Based on Attack Graph

In this paper, we design a correlation algorithm based on AGs that is capable of detecting multiple attack scenarios for forensic analysis. It can be parameterized to adjust the robustness and accuracy. A formal model of the algorithm is presented and an implementation is tested to analyze the different parameters on a real set of alerts from a local network. Intrusion Detection Systems (IDS) have been proposed for years as an efficient security measure and is nowadays widely deployed for securing critical IT-Infrastructures.

III. EXISTING SYSTEM

Cloud users can install vulnerable software on their VMs, which essentially contributes to loopholes in cloud security. The challenge is to establish an effective vulnerability/attack detection and response system for accurately identifying attacks and minimizing the impact of security breach to cloud users. In a cloud system where the infrastructure is

shared by potentially millions of users, abuse and nefarious use of the shared infrastructure benefits attackers to exploit vulnerabilities of the cloud and use its resource to deploy attacks in more efficient ways. Such attacks are more effective in the cloud environment since cloud users usually share computing resources, e.g., being connected through the same switch, sharing with the same data storage and file systems, even with potential attackers. The similar setup for VMs in the cloud, e.g., virtualization techniques, VM OS, installed vulnerable software, networking, etc., attracts attackers to compromise multiple VMs.
The major drawbacks in existing system are:

No detection and prevention framework in a virtual networking environment. Not accuracy in the attack detection from attackers.

IV. Proposed System

This project proposed network Intrusion detection and Countermeasure selection in virtual network systems to establish a defense-in-depth intrusion detection framework. For better attack detection, it incorporates attack graph analytical procedures into the intrusion detection processes. We must note that the design of virtual network system in analysing and detecting attacker does not intend to improve any of the existing intrusion detection algorithms; indeed, it employs a reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, thus preventing zombie VMs.

Since the attacker exploited all the files in the virtual machine while attacking the existing files is again replaced by using data recovery technique by the help third party analyser after detecting and analyzing of the attacker.

V. System Architecture

In this paper as in the figure 1 proposed Network Intrusion detection and Countermeasure selection in virtual network systems is to establish a defense-in-depth intrusion detection framework. For better attack detection, it incorporates attack graph analytical procedures into the intrusion detection processes. We must note that the design of intrusion detection ssytem does not intend to improve any of the existing intrusion detection algorithms; indeed, network intrusion detection employs a reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, thus preventing zombie VMs.

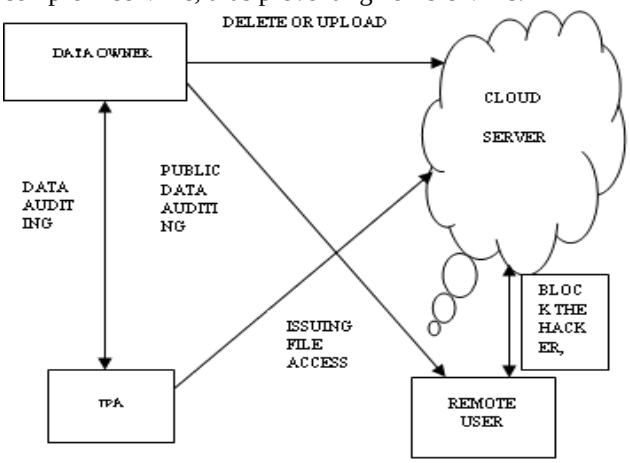

Fig. 1: Architecture of Proposed System

VI. Attack Graph Model Correlation Algorithm

An attack graph alert_correlation is a modelling tool to illustrate all possible multi-stage, multi-host attack paths that are crucial to understand threats and then to decide appropriate countermeasures. In an attack graph, each node represents either precondition or consequence of an exploit. The actions are not necessarily an active attack since normal protocol interactions can also be used for attacks. Attack graph is helpful in identifying potential threats, possible attacks and known vulnerabilities in a cloud system. Since the attack graph provides details of all known vulnerabilities in the system and the connectivity information, we get a whole picture of current security situation of the system where we can predict the possible threats and attacks by correlating detected events or activities. If an event is recognized as a potential attack, we can apply specific countermeasures to mitigate its impact or take actions to prevent it from contaminating the cloud system.

Algorithm 1. Attack Graph Alert_Correlation
Require: alert a_c, SAG, ACG
1: if (ac, is a new alert) then
2: create node ac in ACG
3: $n_1 \leftarrow v_c \in map(a_c)$
4: for all $n_2 \in parent(n_1)$ do
5: create edge (n_2.alert. ac)
6: for all S_i containing a do
7: if a is the last element in S_i then
8: append ac to S_i
9: else
10: create path $S_i+1 =\{ subset(S_i, a), ac\}$
11: end if
12: end for
13: add a_c to n_1.alert
14: end for
15: end if
16: return S

VII. Results

In the server the detection of zombie exploration attack is done using network intrusion detection in virtual network system. Since the exploited memory is analyzed and detected using network intrusion detection method the attacked virtual machine memory can be replaced using data and recovery technique. In this paper, we mainly proposed the zombie exploration attack which is shown in the figure 2

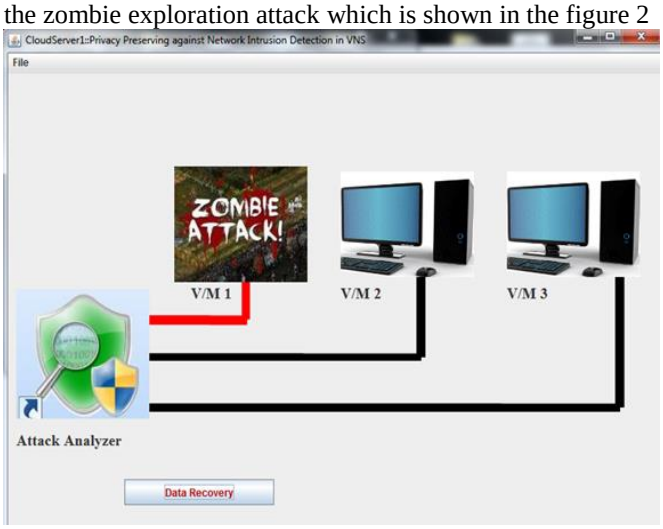

Fig. 2: Result

VIII. CONCLUSIONS

In this work, network intrusion detection against virtual network system is proposed to detect and mitigate collaborative attacks in the cloud virtual networking environment. It utilizes the attack graph model to conduct attack detection and prediction. The proposed solution investigates how to use the programmability of software switches based solutions to improve the detection accuracy and defeat victim exploitation phases of collaborative attacks. The system performance evaluation demonstrates the feasibility of network intrusion detection and shows that the proposed solution can significantly reduce the risk of the cloud system from being exploited and abused by internal and external attackers. It only investigates the network IDS approach to counter zombie explorative attacks.

REFERENCES

[1] Chun-Jen, Pankaj Khatkar, "NICE : Network Intrusion Detection and Counter Measure Selection in Virtual Network System" Proc. IEEE Transactions on Dependable and Secure Computing, vol. 10, no.4 July /August 2013.

[2] 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.

[3] 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. 2010communication and Informatics *(ICCCI '12)*, Jan. 2012.

[4] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "BotHunter: detecting malware infection through IDS-driven dialog correlation," Proc. of 16th USENIX Security Symp. (SS '07), pp. 12:1–12:16, Aug. 2007.

[5] G. Gu, J. Zhang, and W. Lee, "BotSniffer: detecting botnet command and control channels in network traffic," Proc. of 15th Ann. Network and Distributed System Security Symp. (NDSS '08), Feb. 2008.

[6] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," Proc. IEEE Symp. on Security and Privacy, 2002, pp. 273–284.

[7] A. Roy, D. S. Kim, and K. Trivedi, "Scalable optimal counter measure selection using implicit enumeration on attack countermeasure trees," Proc. IEEE Int'l Conf. on Dependable Systems Networks(DSN '12), Jun. 2012.

