ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Discovery of Disturbances in Virtual Network Systems and Countermeasure Selection

Surepalli Suresh Babu
M.tech Student,
Department of Computer Science and Engineering,
VEMU Institute of Technology, Pakala, Chittoor Dist.

B.Rama Ganesh
Associate Professor, Head of the Department,
Department of Computer Science and Engineering,
VEMU Institute of Technology, Pakala, Chittoor Dist.

Abstract:

Now a day's every industry and even some parts of the public sector are using cloud computing, either as a provider or as a consumer. But there are many security issues present in cloud computing environment. There are many possible attacks in cloud computing environment, one such attack is the DoS or its version DDoS attack. Generally, 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 low frequency Vulnerability scanning, multi-step exploitation and compromising identified vulnerable virtual machines as zombies and finally DDoS attacks using the compromised zombies. Inside the cloud system, especially the infrastructure-as-a-Service clouds, the detection of zombie exploration attacks is very difficult.

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 systematic models and reconfigurable virtual network –based countermeasures. This paper provides a short Review on the discovery of disturbances in virtual Network systems and countermeasure selection.

Keywords:

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

1.INTRODUCTION:

Recent studies have shown that users migrating to the cloud consider security as the most important factor. A recent Cloud Security Alliance (CSA) survey shows that among all security issues, abuse and nefarious use of cloud computing is considered as the top security threat [1], 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.

2.RELATED WORK:

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. M. Armbrust et al . addressed that protecting"Business continuity and services availability" from service outages is one of the top concerns in cloud computing systems. 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

DRAWBACKS:

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

3.PROPOSED SYTEM:

In this paper, we propose NICE to Discover of Disturbances in Virtual Network Systems and Countermeasure Selection and establish a defense-in-depth intrusion detection framework. For better attack detection, NICE 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. In general, NICE includes two main phases: (1) deploy a lightweight mirroring-based network intrusion detection agent (NICE-A) on each cloud server to capture and analyze cloud traffic. A NICE-A periodically scans the virtual system vulnerabilities within a cloud server to establish Scenario Attack Graph (SAGs), and then based on the severity of identified vulnerability towards the collaborative attack goals, NICE will decide whether or not to put a VM in network inspection state. (2) Once a VM enters inspection state, Deep Packet Inspection (DPI) is applied, and/or virtual network reconfigurations can be deployed to the inspecting VM to make the potential attack behaviors prominent. NICE significantly advances the current network IDS/IPS solutions by employing programmable virtual networking approach that allows the system to construct a dynamic reconfigurable IDS system. By using software switching techniques, NICE constructs a mirroring-based traffic capturing framework to minimize the interference on users' traffic compared to traditional bump-in-the-wire (i.e., proxy-based) IDS/IPS.

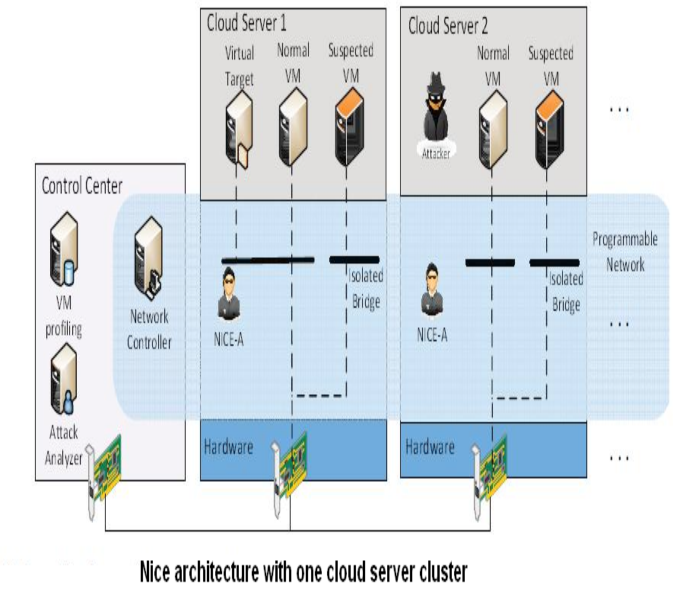

Fig.1: Proposed System Model

» The programmable virtual networking architecture of NICE enables the cloud to establish inspection and quarantine modes for suspicious VMs according to their current vulnerability state in the current SAG. Based on the collective behavior of VMs in the SAG, NICE can decide appropriate actions, for example DPI or traffic filtering, on the suspicious VMs. Using this approach, NICE does not need to block traffic flows of a suspicious VM in its early attack stage. The contributions of NICE are presented as follows:

» We devise NICE, a new multi-phase distributed network intrusion detection and prevention framework in a virtual networking environment that captures and inspects suspicious cloud traffic without interrupting users' applications and cloud services.
» NICE incorporates a software switching solution to quarantine and inspect suspicious VMs for further investigation and protection. Through programmable network approaches, NICE can improve the attack detection probability and improve the resiliency to VM exploitation attack without interrupting existing normal cloud services.
» NICE employs a novel attack graph approach for attack detection and prevention by correlating attack behavior and also suggests effective countermeasures.
» NICE optimizes the implementation on cloud servers to minimize resource consumption.

Our study shows that NICE consumes less computational overhead compared to proxy-based network intrusion detection solutions.

4.IMPLEMENTATION:

The framework of our proposed system has the accompanying modules alongside the following prerequisites.

1.User Module:

In this module, Users are having authentication and security to access the detail which is presented in the ontology system. Before accessing or searching the details user should have the account in that otherwise they should register first. Countermeasure Selection : Countermeasure Selection To illustrate how NICE works, let us consider for example, an alert is generated for node 16 (vAlert = 16) when the system detects LICQ Buffer overflow. After the alert is generated, the cumulative probability of node 16 becomes 1 because that attacker has already compromised that node. This triggers a change in cumulative probabilities of child nodes of node 16. Now the next step is to select the countermeasures from the pool of countermeasures CM.

3. Attack Analyzer:

The major functions of NICE system are performed by attack analyzer, hich includes procedures such as attack graph construction and update, alert correlation and countermeasure selection. The process of constructing and utilizing the cenario Attack Graph (SAG) consists of three phases: information gathering, attack graph construction, and potential exploit path analysis. With this information, attack Paths can be modeled using SAG. Each node in the attack graph represents an exploit by the attacker. Each path from an initial node to a goal node represents a successful attack.

4. False Alarms:

A cloud system with hundreds of nodes will have huge amount of alerts raised by Snort. Not all of these alerts can be relied upon, and an effective mechanism is needed to verify if such alerts need to be addressed.

Since Snort can be programmed to generate alerts with CVE id, one approach that our work provides is to match if the alert is actually related to some vulnerability being exploited. If so, the existence of that vulnerability in SAG means that the alert is more likely to be a real attack. Thus, the false positive rate will be the joint probability of the correlated alerts, which will not increase the false positive rate compared to each individual false positive rate.

Moreover, we cannot keep aside the case of zero day attack where the vulnerability is discovered by the attacker but is not detected by vulnerability scanner. In such case, the alert being real will be regarded as false, given that there does not exist corresponding node in SAG. Thus, current research does not address how to reduce the false negative rate. It is important to note that vulnerability scanner should be able to detect most recent vulnerabilities and sync with the latest vulnerability database to reduce the chance of Zero-day attacks.

5.CONCLUSION:

In this paper, we presented NICE, which is proposed to detect and mitigate collaborative attacks in the cloud virtual networking environment. NICE 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 NICE 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.

NICE only investigates the network IDS approach to counter zombie explorative attacks. In order to improve the detection accuracy, host-based IDS solutions are needed to be incorporated and to cover the whole spectrum of IDS in the cloud system. This should be investigated in the future work. Additionally, as indicated in the paper, we will investigate the scalability of the proposed NICE solution by investigating the decentralized network control and attack analysis model based on current study.

REFERENCES:

[1] Coud Sercurity Alliance, "Top threats to cloud computing v1.0,"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] "Open vSwitch project," http://openvswitch.org, May 2012.

[6] 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.

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

[8] 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.

[9] 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.

[10] "NuSMV: A new symbolic model checker," http://afrodite.itc.it:1024/nusmv. Aug. 2012.

[11] S. H. Ahmadinejad, S. Jalili, and M. Abadi, "A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs," Computer Networks , vol. 55, no. 9, pp. 2221–2240, Jun. 2011.

[12] X. Ou, S. Govindavajhala, and A. W. Appel, "MulVAL: a logic based network security analyzer," Proc. of 14th USENIX Security Symp. , pp. 113–128. 2005.

[13] R. Sadoddin and A. Ghorbani, "Alert correlation survey: framework and techniques," Proc. ACM Int'l Conf. on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services (PST '06) , pp. 37:1–37:10. 2006.

[14] L. Wang, A. Liu, and S. Jajodia, "Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts," Computer Communications , vol. 29, no. 15, pp. 2917–2933, Sep. 2006.

[15] S. Roschke, F. Cheng, and C. Meinel, "A new alert correlation algorithm based on attack graph," Computational Intelligence in Security for Information Systems, LNCS, vol. 6694, pp. 58–67. Springer,2011.

ABOUT AUTHORS:

Surepalli Suresh Babu, received B.Tech degree in the department of Computer Science.a nd Engineering from Global Engineering College, Kadapa in 2012 Currently he is pursuing his master's degree from Vemu Institute Of Technology, Pakala, Chittoor Dist, A.P, JNTUA in the department of Computer Science. His current interests include Computer Networks Cloud Computing and Data Mining.

Mr. B. Rama Ganesh is currently working as Associate professor, HOD, Dept of CSE in Vemu institute of technology Pakala, Chittoor Dist, A.P, JNTUA. He received M.Tech degree from St. Mary's college of Engineering; Hyderabad in 2009.He is currently doing his PhD work at Rayalaseema University, kurnool on subjects. His current interests include Computer Networks,Microprocessors and Computer architecture Multimedia Technology.