

7. NICE System Component

- Nice-D
- VM Profiling
- Attack Analyzer
- Network Controller

7.1 Nice-D

The NICE-D is a Network-based Intrusion Detection System (NIDS) with dynamic IDS installed in each cloud server. It scans the traffic going through the bridges that control all the traffic among VMs and in/out from the physical cloud servers. It will sniff a mirroring port on each virtual bridge in the Open vSwitch. Each bridge forms an isolated subnet in the virtual network and connects to all related VMs. 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's more efficient to scan the traffic in cloud server since all traffic in the cloud server needs go through it; however our design is independent to the installed VM. The false alarm rate could be reduced through our architecture design.

7.2 VM Profiling

Virtual machines in the cloud can be profiled to get precise information about their state, services running, open ports, etc. One major factor that counts towards a VM profile is its connectivity with other VMs. Also required is the knowledge of services running on a VM so as to verify the authenticity of alerts pertaining to that VM. An attacker can use port scanning program to perform an intense examination of the network to look for open ports on any VM. So information about any open ports on a VM and the history of opened ports plays a significant role in determining how vulnerable the VM is. All these factors combined will form the VM profile. VM profiles are maintained in a database and contain comprehensive information about vulnerabilities, alert and traffic.

7.3 Attack Analyzer

The major functions of NICE system are performed by attack analyzer, which includes procedures such as attack graph construction and update, alert correlation and countermeasure selection. The process of constructing and utilizing the Scenario 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. The Attack Analyzer also handles alert correlation and analysis operations. This component has two major functions: (1) constructs Alert Correlation Graph (ACG), (2) provides threat information and appropriate countermeasures to network controller for virtual network reconfiguration. NICE attack graph is constructed based on the following information: *Cloud system information, Virtual network topology and configuration information, Vulnerability information*

7.4 Network Controller

The network controller is a key component to support the programmable networking capability to realize the virtual network reconfiguration. In NICE, we integrated the control functions for both OVS and OFS into the network controller that allows the cloud system to set security/filtering rules in an integrated and comprehensive manner. The network controller is responsible for collecting network information of current Open Flow network and provides input to the attack analyzer to construct attack graphs. In NICE, the network control also consults with the attack analyzer for the flow access control by setting up the filtering rules on the corresponding OVS and OFS. Network controller is also responsible for applying the countermeasure from attack analyzer. Based on *VM Security Index* and severity of an alert, countermeasures are selected by NICE and executed by the network controller.

8. Conclusion

NICE-D for cloud system work better than the existing system NICE-A. NICE-A covered all possible work for the VM over cloud but did not considered the improvement to the intrusion detection algorithm. In this paper we proposed the new dynamic intrusion detection algorithm which performs better than the existing signature based SNORT.

References

- [1] Chun-Jen Chung, Student Member, IEEE, Pankaj Khatkar, Student Member, IEEE, Tianyi Xing, Jeongkeun Lee, Member, IEEE, and Dijiang Huang Senior Member, IEEE, "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems"- IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, 2013.
- [2] Cloud Security Alliance, "Top Threats to Cloud Computing v1.0," <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>, Mar. 2010.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] "Open vSwitch Project," <http://openvswitch.org>, May 2012.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] Michael Armbrust, Armando Fox, Rean Griffith “Above the Clouds: A View of Cloud Computing” Tech. Rep. UCB/EECS-2009-28, EECS Department, U.C. Berkeley, Feb 2012.
- [11] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande “Intrusion Detection System for Cloud Computing “International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012.
- [12] J. Sasi Devi, R. Sugumar “Host Based Intrusion Detection to Prevent VirtualNetwork System from Intruders in Cloud” International Journal of Science and Research (IJSR) 2014