

SECURE NETWORK ID AND ATTACK MEASURE SELECTION IN VIRTUAL NETWORK

S.Uvaraj*

S.Suresh**

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. The proposed framework leverages Open Flow network programming APIs to build a monitor and control plane over distributed programmable virtual switches in order to significantly improve attack detection and mitigate attack consequences. The system and security evaluations demonstrate the efficiency and effectiveness of the proposed solution.

Keywords - Network Security, Cloud Computing, Intrusion Detection, Attack Graph, Zombie Detection

* M.E/CSE, Arulmigu Meenakshi Amman College of Engineering, Kanchipuram, India

** B.Tech/IT, Sri Venkateswara College of Engineering, Chennai, India

I. INTRODUCTION

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. 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 [2], 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 [3]. 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 [4]. 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.

In this paper, we propose NICE (Network Intrusion detection and Countermeasure sElection in virtual network systems) to 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 behaviours prominent.

The rest of paper is organized as follows. Section II presents the related work. Section III describes system approach and implementation. System models are described in Section IV describes the approach to hardening the network in NICE. The proposed NICE is presented in Section V and Section VI evaluates NICE in terms of network performance and security. Finally, Section VII describes future work and concludes this paper.

II. RELATED WORKS

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.

Intrusion Detection System (IDS) and firewall are widely used to monitor and detect suspicious events in the network. However, the false alarms and the large volume of raw alerts from IDS are two major problems for any IDS implementations. In order to identify the source or target of the intrusion in the network, especially to detect multi-step attack, the alert correction is a must-have

tool. The primary goal of alert correlation is to provide system support for a global and condensed view of network attacks by analyzing raw alerts [13]. Many attack graph based alert correlation techniques have been proposed recently. L. Wang et al. [14] devised an in-memory structure, called queue graph (QG), to trace alerts matching each exploit in the attack graph. However, the implicit correlations in this design make it difficult to use the correlated alerts in the graph for analysis of similar attack scenarios. Roschke et al. [15] proposed a modified attack-graph-based correlation algorithm to create explicit correlations only by matching alerts to specific exploitation nodes in the attack graph with multiple mapping functions, and devised an alert dependencies graph (DG) to group related alerts with multiple correlation criteria. [17] proposed a Bayesian attack graph (BAG) to address dynamic security risk management problem and applied a genetic algorithm to solve countermeasure optimization problem.

III. NICE MODELS

In this section, we describe how to utilize attack graphs to model security threats and vulnerabilities in a virtual networked system, and propose a VM protection model based on virtual network reconfiguration approaches to prevent VMs from being exploited.

3.1 Threat Model

In our attack model, we assume that an attacker can be located either outside or inside of the virtual networking system. The attacker's primary goal is to exploit vulnerable VMs and compromise them as zombies. Our protection model focuses on virtual-network-based attack detection and reconfiguration solutions to improve the resiliency to zombie explorations.

Our work does not involve host-based IDS and does not address how to handle encrypted traffic for attack detections. Our proposed solution can be deployed in an Infrastructure- s-a-Service (IaaS) cloud networking system, and we assume that the Cloud Service Provider (CSP) is benign. We also assume that cloud service users are free to install whatever operating systems or applications.

3.2 Attack Graph Model

An attack graph is a modeling tool to illustrate all possible multi-stage, multi-host attack paths that are crucial to understand threats and then to decide appropriate countermeasures [22]. In an attack graph, each node represents either precondition or consequence of an exploit.

Attack graph is helpful in identifying potential threats, possible attacks and known vulnerabilities in a cloud system.

Definition 1 (Scenario Attack Graph). An Scenario Attack Graph is a tuple $SAG = (V, E)$, where,

1. $V = NC \cup ND \cup NR$ denotes a set of vertices that include three types namely conjunction node NC to represent exploit, disjunction node ND to denote result of exploit, and root node NR for showing initial step of an attack scenario.

2. $E = Epre \cup Epost$ denotes the set of directed edges. An edge $e \in Epre \cup ND \cup NC$ represents that ND must be satisfied to achieve NC. An edge $e \in Epost \cup NC \cup ND$ means that the consequence shown by ND can be obtained if NC is satisfied.

Node $vc \in NC$ is defined as a three tuple (Hosts; vul; alert) representing a set of IP addresses, vulnerability information such as CVE [23], and alerts related to vc, respectively. ND behaves like a logical OR operation and contains details of the results of actions.

NR represents the root node of the scenario attack graph. For correlating the alerts, we refer to the approach described in [15] and define a new Alert Correlation Graph (ACG) to map alerts in ACG to their respective nodes in SAG. To keep track of attack progress, we track the source and destination IP addresses for attack activities.

Definition 2 (Alert Correlation Graph).

An ACG is a three tuple $ACG = (A; E; P)$, where

1. A is a set of aggregated alerts. An alert $a \in A$ is a data structure (src; dst; cls; ts) representing source IP address, destination IP address, type of the alert, and timestamp of the alert respectively.

2. Each alert a maps to a pair of vertices (vc; vd) in SAG using map (a) function,

3. E is a set of directed edges representing correlation between two alerts

4. P is set of paths in ACG.

Algorithm 1 AlertCorrelation

Require: alert ac, SAG, ACG

if (ac is a new alert) **then** create node ac in ACG

$n1 \leftarrow vc \in \text{map}(ac)$

for all $n2 \text{ parent}(n1)$ **do**

create edge (n2, alert, ac)

```

for all Si containing a do
if a is the last element in Si then
  append ac to Si
    else
  create path Si+ 1 = { subset(Si a)ac }
    end if
end for
  add ac to n1 alert
end for
end if
return S

```

Definition 3 (VM State). Based on the information gathered from the network controller, VM states can be defined as following:

1. Stable: there does not exist any known vulnerability on the VM.
2. Vulnerable: presence of one or more vulnerabilities on a VM, which remains unexploited.
3. Exploited: at least one vulnerability has been exploited and the VM is compromised.
4. Zombie: VM is under control of attacker.

IV. NICE SYSTEM DESIGN

In this section, we first present the system design overview of NICE and then detailed descriptions of its components.

4.1 System design overview

The proposed NICE framework is illustrated in Figure 1. It shows the NICE framework within one cloud server cluster. Major components in this framework are distributed and light-weighted NICE-A on each physical cloud server, a network controller, a VM profiling server, and an attack analyzer. The latter three components are located in a centralized control center connected to software switches on each cloud server (i.e., virtual switches built on one or multiple Linux software bridges).

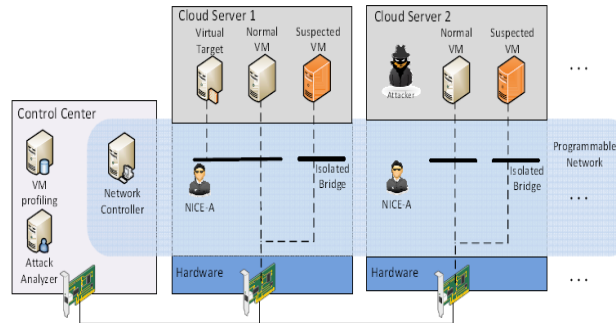


Fig 1. NICE framework within one cloud server cluster

4.2 SYSTEM COMPONENTS

In this section we explain each component of NICE.

4.2.1 NICE-A

The NICE-A is a Network-based Intrusion Detection System (NIDS) agent installed in either dom0 or domU in each cloud server. It scans the traffic going through Linux bridges that control all the traffic among VMs and in/out from the physical cloud servers. NICEA is a software agent implemented in each cloud server connected to the control center through a dedicated and isolated secure channel, which is separated from the normal data packets using OpenFlow tunneling or VLAN approaches. The network controller is responsible for deploying attack countermeasures based on decisions made by the attack analyzer.

4.2.2 VM Profiling

Virtual machines in the cloud can be profiled to get precise information about their state, services running, open ports, etc.

VM profiles are maintained in a database and contain comprehensive information about vulnerabilities, alert and traffic. The data comes from:

- ❖ Attack graph generator: while generating the attack graph, every detected vulnerability is added to its corresponding VM entry in the database.
- ❖ NICE-A: the alert involving the VM will be recorded in the VM profile database.
- ❖ Network controller: the traffic patterns involving the VM are based on 5 tuples (source MAC address, destination MAC address, source IP address, destination IP address, protocol). We can have traffic pattern where packets emanate from a single IP and are delivered to multiple destination IP addresses, and vice-versa.

4.2.3 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 modelled using SAG.

In summary, NICE attack graph is constructed based on the following information:

- ❖ Cloud system information is collected from the node controller and VM's Virtual Interface (VIF) information.
- ❖ Virtual network topology and configuration information is collected from the network controller, every VM's IP address, MAC address, port information, and traffic flow information.
- ❖ Vulnerability information is generated by both on demand vulnerability scanning.

4.2.4 Network Controller

The network controller is a key component to support the programmable networking capability to realize the virtual network reconfiguration feature based on Open-Flow protocol [20]. In NICE, within each cloud server there is a software switch, for example, Open vSwitch (OVS) [5], which is used as the edge switch for VMs to handle traffic in & out from VMs. The network controller is responsible for collecting network information of current OpenFlow network and provides input to the attack analyzer to construct attack graphs.

V. MITIGATION AND COUNTERMEASURES

In this section, we present the methods for selecting the countermeasures for a given attack scenario. The countermeasure serves the purpose of 1) protecting the target VMs from being compromised; and 2) making attack behavior stand prominent so that the attackers' actions can be identified.

5.1 Mitigation Strategies

Based on the security metrics defined in the previous subsection, NICE is able to construct the mitigation strategies in response to detected alerts. First, we define the term countermeasure pool as follows:

Definition 4 (Countermeasure Pool).

A countermeasure pool $CM = (cm_1; cm_2; \dots; cm_n)$ is a set of countermeasures. Where

1. Cost is the unit that describes the expenses required to apply the countermeasure in terms of resources and operational complexity, and it is defined in a range from 1 to 5, and higher metric means higher cost;
2. intrusiveness is the negative effect that a countermeasure brings to the Service Level Agreement (SLA) and its value ranges from the least intrusive (1) to the most intrusive (5), and the value of intrusiveness is 0 if the countermeasure has no impacts on the SLA;
3. Condition is the requirement for the corresponding countermeasure;
4. Effectiveness is the percentage of probability changes of the node, for which this countermeasure is applied.

TABLE 1
Possible Countermeasure Types

No.	Countermeasure	Intrusiveness	Cost
1	Traffic redirection	3	3
2	Traffic isolation	4	2
3	Deep Packet Inspection	3	3
4	Creating filtering rules	1	2
5	MAC address change	2	1
6	IP address change	2	1
7	Block port	4	1
8	Software patch	5	4
9	Quarantine	5	2
10	Network reconfiguration	0	5
11	Network topology change	0	5

5.2 Countermeasure selection

Algorithm 2 presents how to select the optimal countermeasure for a given attack scenario. Input to the algorithm is an alert, attack graph G , and a pool of countermeasures CM . The algorithm starts by selecting the node v_{Alert} that corresponds to the alert generated by a NICE-A. The countermeasure which when applied on a node gives the least value of ROI, is regarded as the optimal countermeasure. Finally, SAG and ACG are also updated before terminating the algorithm.

Algorithm 2 Countermeasure Selection

Require: Alert; $G(E; V)$; CM

Let v_{Alert} = Source node of the Alert

if Distance to Target(v_{Alert}) > threshold then

Update ACG

Return

end if

Let $T = \text{Descendant}(v_{Alert}) \cup v_{Alert}$

Set $\text{Pr}(v_{Alert}) = 1$

Calculate Risk Prob(T)

Let $\text{benefit}[jTj; jCMj] = \emptyset$

for each $t \in T$ do

for each $cm \in CM$ do

if $cm:\text{condition}(t)$ then

$\text{Pr}(t) = \text{Pr}(t) \cdot (1 - cm:\text{effectiveness})$

Calculate Risk Prob($\text{Descendant}(t)$)

$\text{benefit}[t; cm] = \text{Pr}(\text{target node}) \cdot (7)$

end if

end for

end for

Let $\text{ROI}[jTj; jCMj] = \emptyset$

for each $t \in T$ do

for each $cm \in CM$ do

$\text{ROI}[t; cm]$

end for

end for

Update SAG and Update ACG

return Select Optimal CM(ROI)

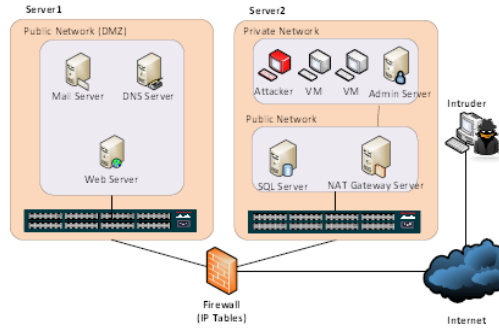


Fig. 3. Virtual network topology for security evaluation.

TABLE 2
Vulnerabilities in the virtual networked system.

Host	Vulnerability	Node	CVE	Base Score
VM group	LICQ buffer overflow	10	CVE 2001-0439	0.75
	MS Video ActiveX Stack buffer overflow	5	CVE 2008-0015	0.93
	GNU C Library loader flaw	22	CVE-2010-3847	0.69
Admin Server	MS SMV service Stack buffer overflow	2	CVE 2008-4050	0.93
	OpenSSL uses predictable random variable	15	CVE 2008-0166	0.78
Gateway server	Heap corruption in OpenSSH	4	CVE 2003-0693	1
	Improper cookies handler in OpenSSH	9	CVE 2007-4752	0.75
	Remote code execution in SMTP	21	CVE 2004-0840	1
Mail server	Squid port scan	19	CVE 2001-1030	0.75
	WebDAV vulnerability in IIS	13	CVE 2009-1535	0.76

VI. PERFORMANCE EVALUATION

In this section we present the performance evaluation of NICE. Our evaluation is conducted in two directions: the security performance, and the system computing and network reconfiguration overhead due to introduced security mechanism.

6.1 Security Performance Analysis

To demonstrate the security performance of NICE, we created a virtual network testing environment consisting of all the presented components of NICE.

6.1.1 Environment and Configuration

To evaluate the security performance, a demonstrative virtual cloud system consisting of public (public virtual servers) and private (VMs) virtual domains is established as shown in Figure 3. Cloud Servers 1 and 2 are connected to Internet through the external firewall.

6.1.2 Attack Graph and Alert Correlation

6.2 NICE System Performance

We evaluate system performance to provide guidance on how much traffic NICE can handle for one cloud server and use the evaluation metric to scale up to a large cloud system. In a real cloud system, traffic planning is needed to run NICE, which is beyond the scope of this paper. Due to the space limitation, we will investigate the research involving multiple cloud clusters in the future.

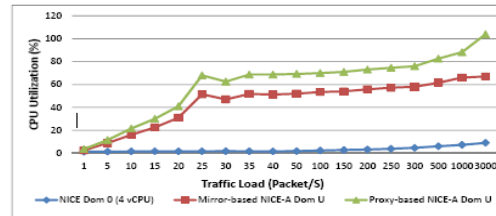


Fig. 9. CPU utilization of NICE-A.

VII. CONCLUSION AND FUTURE WORK

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] R. Sadoddin and A. Ghorbani, "Alert correlation survey: framework and techniques," in Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services, ser. PST '06. New York, NY, USA: ACM, 2006, pp. 37:1–37:10.
- [2] S. Roschke, F. Cheng, and C. Meinel, "A new alert correlation algorithm based on attack graph," in Computational Intelligence in Security for Information Systems, ser. Lecture Notes in Computer Science. Springer, 2011, vol. 6694, pp. 58–67.
- [3] Cloud Security Alliance, "Top threats to cloud computing v1.0," <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>, March 2010.
- [4] 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," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.
- [5] B. Joshi, A. Vijayan, and B. Joshi, "Securing cloud computing environment against DDoS attacks," in Computer Communication and Informatics (ICCCI), 2012 International Conference on, Jan. 2012, pp.1 –5.
- [6] 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.
- [7] "Open vSwitch project," <http://openvswitch.org>, May 2012.
- [8] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, "Detecting spam zombies by monitoring outgoing messages," Dependable and Secure Computing, IEEE Transactions on, vol. 9, no. 2, pp. 198 –210, Apr. 2012.
- [9] "Metasploit," <http://www.metasploit.com>.
- [10] <http://www.fastandeasyhacking.com>.