International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

ISRV: Intrusion Detection, Selection of Counter Measures and Recovery of Virtual Network Systems

Vinod Kumar[1], Syeda Asra[2], Yallappa Meti[3]

[1, 2, 3]Appa Institute of Engineering and Technology, Vivesvaraya Technological University, Jnana Sangam, Belgaum 590018

Abstract: ***A considerable lot of the computer infrastructure are progressively vulnerable to attacks (assaults), since intrusion detection is essential however shockingly deficient. So we have to design and implement a powerful detection and reaction techniques to bypass intrusions when they are detected. This intrusion and detection strategy is in view of distinctive sorts of counter-measures. The principle thought is to design and develop a decision support tool to help the administrator to pick the suitable counter-measure when an intrusion is detected. Cloud computing is another developing strategy in computer oriented services. This framework have some distributed system, as per these likenesses of cloud computing additionally utilizes the components of virtual networking environment. And it provides the Data recovery of the Cloud Server when attacker attacks the Cloud; here it uses the basic data recovery algorithm by taking the backup of Cloud Server.***

Keywords: Network security, cloud computing, intrusion detection, attack graph, zombie detection, Data recovery.

1. Introduction

Cloud computing is the utilization of computing resources (hardware and software) that are conveyed as a services over a network (ordinarily the Internet). Cloud computing is a model for empowering helpful, on demand network access to a mutual pool of configurable processing resources (e.g., networks, servers, stockpiling, applications and services) that can be quickly provisioned and discharged with minimal administration exertion or service provider association.

Cloud computing environment is a interaction between two or more Cloud computing destinations which offers distinctive reckonings. End users access cloud-based applications through a web program or a light-weight desktop or versatile application while the business programming and user's information are stored on servers at a remote area. Defenders guarantee that Cloud computing permits organizations to evade forthright infrastructure cost, and concentrate on ventures that separate their business rather than infrastructure. Proponents additionally assert that Cloud computing permits undertakings to get their applications up and running speedier, with enhanced manageability and less maintenance, and empowers IT to all the more quickly modify resources to meet fluctuating and capricious business request. A cloud is characterized as a large-scale distributed computing model that is driven by economies of scale, in which a pool of disconnected, virtualized, alertly versatile, managed computing power, stockpiling, platforms, and services are conveyed on demand to outside users over the Internet.

What's more, with applications facilitated midway, updates can be released without the requirement for users to install new software. One disadvantage of SaaS is that the users' information are put away on the cloud supplier's server.

Subsequently, there could be unauthorized access to the information. Cloud computing depends on sharing of assets to accomplish rationality and economics of scale like an utility like the power matrix more than a network. At the establishment of Cloud computing is the more extensive idea of converged infrastructure and shared services. Cloud computing depends on sharing of assets to accomplish rationality and economies of scale. VM Management for Cross Cloud Computing Environment

1.1 Characteristics of Cloud computing

Cloud computing displays the accompanying key qualities:

1) Agility enhances with users' capacity to re-procurement mechanical framework assets.
2) Application programming interface (API) openness to software that empowers machines to collaborate with cloud programming in the same way that a customary user interface (e.g., a PC desktop) encourages communication in the middle of people and computers.
3) Cost is asserted to be decreased, and in a public cloud delivery model capital expenditure is changed over to operational expenditure. This is indicated to lower boundaries to entry, as infrastructure is normally given by an third-party and does not should be obtained for one-time or rare intensive computing tasks.
4) Device and location independence empower users to get to systems utilizing a web browser regardless of their location or what gadget they are using (e.g., PC, cellular phone). As framework is off-webpage (normally gave by an outsider) and got to through the Internet, users can unite from anyplace.
5) Virtualization technology permits servers and storage devices to be shared and use be expanded. Applications can be effortlessly relocated starting with one physical server then onto the next.
6) Multitenancy empowers sharing of assets and expenses over a vast pool of users.
7) Reliability is enhanced if different excess locales are utilized, which makes all around composed Cloud computing suitable for business progression and calamity recuperation.

8) Scalability and flexibility through element ("on-interest") provisioning of resources on a fine-grained, self-service basis real time, without users needing to engineer for crest burdens VM Management for Cross Cloud Computing Environment
9) Performance is observed reliable and loosely coupled architectures are developed utilizing web services as the system interface.
10) Maintenance of Cloud computing applications is simpler, in light of the fact that they don't shouldbe introduced on every user's PC and can be gotten to from better places.

2. Literature Survey

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 [2], 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 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. By using software switching techniques [5], 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. The work by Duan et al. [6] focuses on the detection of compromised machines that have been recruited to serve as spam zombies. BotHunter [7] detects compromised machines based on the fact that a thorough malware infection process has a number of well-defined stages that allow correlating the intrusion alarms triggered by inbound traffic with resulting outgoing communication patterns. BotSniffer [8] exploits uniform spatial-temporal behavior characteristics of compromised machines to detect zombies by grouping flows according to server connections and searching for similar behavior in the flow. Sheyner et al. [9] proposed a technique based on a modified symbolic model checking NuSMV [10] and Binary Decision Diagrams (BDDs) to construct attack graph. Their model can generate all possible attack paths, however, the scalability is a big issue for this solution.

3. Methodology

System Design first present the system outline review of ISRV and afterward itemized depictions of its components.

System outline diagram

The proposed ISRV system is represented in the figure. It demonstrates the ISRV system inside of one cloud server cluster. Significant components System are distributed and light-weighted ISRV-A on each physical cloud server, a network controller, a VM profiling server, and an attack analyzer.

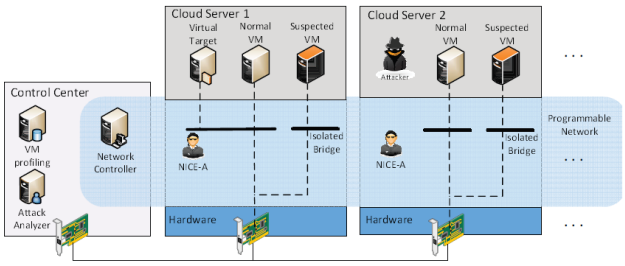

Figure 3.1: System Design

The recent three parts are situated in a centralized control center associated with software switches on every cloud server (i.e., virtual switches based on one or different Linux software scaffolds). ISRV-A is a software specialist executed in every cloud server joined with the control center through a dedicated and isolated secure channel, which is isolated from the typical data parcels utilizing OpenFlow tunneling or VLAN approaches. The network controller is in charge of sending attack countermeasures in light of choices made by the attack analyzer.

Attack Analyzer

The real elements of ISRV system are performed by attack analyzer, which incorporates techniques, for example, attack graph construction and update, alert correlation and countermeasure selection. The procedure of developing and using the Scenario Attack Graph (SAG) comprises of three platforms: data gathering, attack graph construction, and potential path analysis. With this data, attack paths can be displayed utilizing SAG. Every node in the attack graph speaks to an adventure by the attacker. Every path from an initial node to an objective node speaks to an effective attack. In synopsis, ISRV attack graph is developed taking into account the accompanying data:

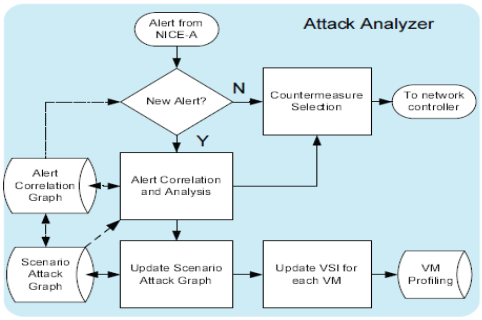

Figure 3.2: Attack Analyzer

Network Controller

The Network controller is a key segment to backing the programmable systems service ability to understand the virtual system reconfiguration highlight in light of Open-Flow protocol. In ISRV, inside of every cloud server there is a software switch, for instance, Open vSwitch (OVS), which

is utilized as the edge switch for VMs to handle activity in & out from VMs.

Network controller is additionally in charge of applying the countermeasure from attack analyzer. In light of *VM Security Index* and seriousness of a ready, countermeasures are chosen by ISRV and executed by the Network controller. In the event that an extreme caution is activated and recognizes some known attack s, or a VM is distinguished as a zombie, the Network controller will hinder the VM quickly. A caution with medium danger level is activated by a suspicious bargained VM. Countermeasure in such case is to put the suspicious VM with misused state into isolate mode and divert every one of its streams to ISRVA Deep Packet Inspection (DPI) mode. A caution with a minor risk level can be produced because of the vicinity of a helpless VM. For this case, to catch the VM's typical movement, suspicious activity to/from the VM will be put into investigation mode, in which activities, for example, confining its stream data transfer capacity and changing system designs will be taken to drive the attack investigation conduct to emerge.

4. Results

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

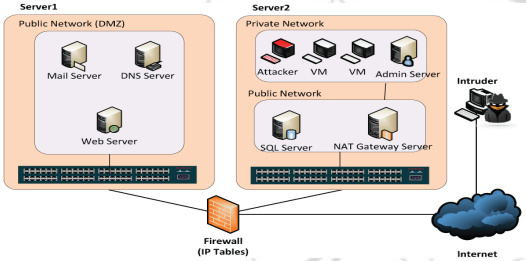

Figure 4.1: Virtual network topology for security Evaluation

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
Gateway server	OpenSSL uses predictable random variable	15	CVE 2008-0166	0.78
	Heap corruption in OpenSSH	4	CVE 2003-0693	1
	Improper cookies handler in OpenSSH	9	CVE 2007-4752	0.75
Mail server	Remote code execution in SMTP	21	CVE 2004-0840	1
	Squid port scan	19	CVE 2001-1030	0.75
Web server	WebDAV vulnerability in IIS	13	CVE 2009-1535	0.76

Attack Graph and Alert Correlation

Creating an attack graph requires knowledge of network connectivity, running services, and their vulnerability information. This information is provided to the attack graph generator as the input. Whenever a new vulnerability is discovered or there are changes in the network connectivity and services running through them, the updated information is provided to attack graph generator and old attack graph is updated to a new one. SAG provides information about the possible paths that an attacker can follow. ACG serves the purpose of confirming attackers' behavior, and helps in determining false positive and false negative. ACG can also be helpful in predicting attackers' next steps.

Countermeasure Selection

To illustrate how NICE works, let us consider, for example, an alert is generated for node 16 (vAlert ¼ 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. If the countermeasure CM4: Create filtering rules is applied to node 5 and we assume that this countermeasure has effectiveness of 85 percent, the probability of node 5 will change to 0.1164, which causes change in probability values of all child nodes of node 5 thereby accumulating to a decrease of 28.5 percent for the target node 1.

5. Conclusion

In this paper, we introduced ISRV, which is proposed to identify and mitigate shared attacks in the cloud virtual networking environment. ISRV uses the attack graph model to lead attack detection and prediction. The proposed solution researches how to utilize the programmability of software switches-based solutions for enhance the detection accuracy and annihilation victim exploitation phases of synergistic attacks. The system performance assessment exhibits the plausibility of ISRV and demonstrates that the proposed solution can altogether diminish the risk of the cloud system from being exploited and abused by internal and external attackers.

6. Future Scope

ISRV only investigates the network IDS approach to counter zombie explorative attacks. 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 ISRV solution by investigating the decentralized network control and attack analysis model based on current study.

References

[1] CoudSecurity Alliance, "Top Threats to Cloud Computing v1.0," https://cloudsecurityalliance.org/topthreats/csathreats. v1.0.pdf, Mar. 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 Comm., vol. 53, no. 4, pp. 50-58, Apr. 2010.
[3] 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.
[4] 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.
[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] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, "Automated Generation and Analysis of Attack Graphs," Proc. IEEE Symp. Security and Privacy, pp. 273-284, 2002,
[8] "NuSMV: A New Symbolic Model Checker," http://afrodite.itc. it:1024/nusmv. Aug. 2012.
[9] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph- based network vulnerability analysis," Proc. 9th ACM Conf. Computer and Comm. Security (CCS '02), pp. 217-224, 2002.
[10] P. Mell, K. Scarfone, and S. Romanosky, "Common Vulnerability Scoring System (CVSS)," http://www.first.org/cvss/cvss-guide.html, May 2010.

Author Profile

Vinod Kumar received the B.E degree in computer science from Visvesvaraya Technological University. He is currently working toward the M.Tech degree in the Appa Institute of Engineering and Technology at Visvesvaraya Technological University.

Yallappa Meti received the B.E degree in computer science from VisvesvarayaTechnological University. He is currently working toward the M.Tech degree in the Appa Institute of Engineering and Technology at VisvesvarayaTechnological University.