NETWORK THREAT DIAGNOSIS AND COUNTERMEASURES IN CLOUD SYSTEM

S.P. MALARVIZHI, P.SUNDARAM, S.BHASKAR

Department of Computer Science and Engineering,
AVS Engineering College, Salem.

Abstract

In a cloud computing the security issues day by day increased. To overcome this security issues we handle lot of research and development. In this paperCloud security is one of most important issues in cloud system. Attackers to search the possibility of attack in cloud system and to send the report to Distributed Denial-of-Service (DDoS).DDoS attacks involve multistep exploitation, low-frequency vulnerability scanning, and identified possibility attacks of virtual machines as zombies, In DDoS attacks through the compromised zombies. Within the cloud system, the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie the possibility of attacks is very high. Cloud users may install the vulnerable applications in virtual machines. To prevent vulnerable virtual machines in the cloud, we propose multiphase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE, based on attack graph-based analytical models and reconfigurable virtual network-based countermeasures. In proposed system Open Flow network programming APIs to build a monitor and control plane over distributed programmable virtual switches and to improve attack detection and possibility of security is high. The system and security to improve the efficiency and effectiveness of the proposed solution.

Index Terms: cloud computing,DDoS attack, intrusion detection, zombie detection,.

Introduction

Cloud computing involves a large number of computers connected through a real- time network (Internet). It describes a variety of computing concepts. It has the ability to rum program or application on many computers at a time. It refers to network- based services; virtual servers do not exit physically. Cloud computing is a type of Internet- based computing. High performance computing is the goal of cloud computing.

Cloud Computing is used to both the applications services over the Internet and the hardware and systems software in cloud services. Three types of services used in cloud systems. To provides security and Privacy of application in cloud is called Software as a Services (SaaS).to be build own applications in cloud Platform as a services (PaaS). To product low level data also in cloud system is called Infrastructure as a services (IaaS).In a Security Level Agreements (SLA) is a part of service between the customer and provider in formally defined the level of services.

A recent Cloud Security Alliance (CSA) survey shows that among all security issues, misuse the data and wrongly use of cloud computing is considered as the top security threat [1], where system administrators have full control over the host machines, vulnerabilities can be detected and added a small computer program in existing system by the system administrator in a centralized type. However, adding a small program in existing system in cloud, where cloud users usually have the only one person and group of people to control software installed on their managed Virtual Machines, may not work effectively and can break the service level agreement (SLA). In cloud users can install vulnerable software on their Virtual Machines, which relating to the most important ideas to contribute in a small mistake in cloud security.

The challenge is to establish an effective vulnerability or attack detection and response system for accurately identifying attacks and minimizing the impact of security breach to cloud users. 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, misuse and wrongly use of the shared infrastructure benefits attackers to exploit vulnerabilities of the cloud and use its resource to effective way attacks in more efficient ways. Such attacks are more effective in the cloud environment because cloud users usually share computing resources.

Methodology

NICE, a new multiphase distributednetwork intrusion detection and prevention frameworkin a virtual networking environment thatcaptures and inspects suspicious cloud traffic withoutinterrupting user applications and cloud services.NICE incorporates a software switching solution toquarantine and inspect suspicious VMs for furtherinvestigation and protection. Through programmablenetwork approaches, NICE can improve theattack detection probability and improve the resiliencyto VM exploitation attack without interruptingexisting normal cloud services.NICE employs a novel attack graph approach forattack detection and prevention by correlatingattack behavior and also suggests effective countermeasures.NICE optimizes the implementation on cloudservers to minimize resource consumption. Ourstudy shows that NICE consumes less computationaloverhead compared to proxy-based networkintrusion detection solutions.

NICE Models

1 Threat Model

The attacker's primary goal is to exploit vulnerableVMs and compromise them as zombies. In protectionmodel focuses on virtual-network-based attack detectionand reconfiguration solutions to improve the resiliency tozombie explorations. It does not involve host-basedIDS and does not address how to handle encrypted trafficfor attack detections.In proposed solution can be deployed in an Infrastructure-as-a-Service (IaaS) cloud networking system, andthat the Cloud Service Provider (CSP) is caring.In that cloud service users are free to installwhatever operating systems or applications to want, even if such action may introduce vulnerabilities to theircontrolled VMs.

2 Attack Graph Model

An attack graph is a modeling tool to demonstrate all possiblemultistage, multihost attack paths that are crucial tounderstand threats and then to decide appropriate countermeasures[22]. In an attack graph, each node representseither precondition or consequence of an exploit. Theactions are not necessarily an active attack because normalprotocol interactions can also be used for attacks. Attackgraph is helpful in identifying potential threats, possibleattacks, and known vulnerabilities in a cloud system.

3 VM Protection Model

The VM protection model of NICE consists of a VMprofiler, a security indexer, and a state monitor. To specifysecurity index for all the VMs in the network dependingupon various factors like connectivity, the number ofvulnerabilities present and their impact scores. The impactscore of a vulnerability, as defined by the CVSS guide [24],helps to judge the confidentiality, integrity, and availabilityimpact of the vulnerability being exploited. Connectivitymetric of a VM is decided by evaluating incoming andoutgoing connections.

EXISTING SYSTEM

Attackerscandiscover vulnerabilities of a cloud system and negotiation effective machines to organize further large-scale Distributed Denial-of-Service (DDoS). DDoS attacks usually involve early stage actions such as multistep management,low-frequency defencelessness scanning, and compromising identified defenceless effective machines as zombies, and finally DDoS attacks through the negotiation zombies. Within the cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie searching attacks is very difficult. This is because cloud users may install defenceless applications on their virtual machines.

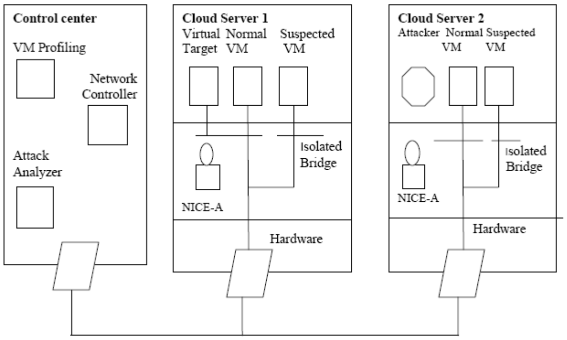


Fig 3.1 NICE Architecture

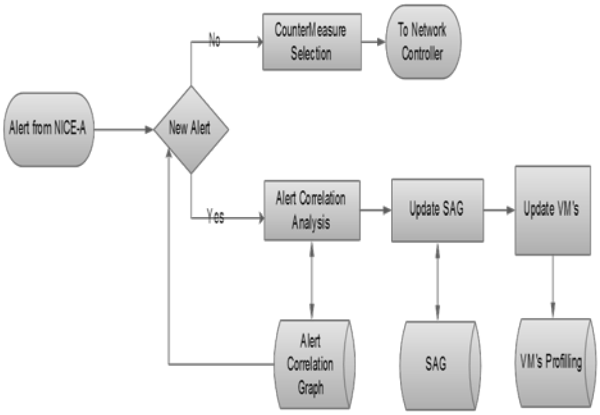
In top threats in cloud computing attackers can misuse the data and wrongly used. By abusing usage models, spammers, wicked code authors, and other criminals have been conducting their activities. Iass severs for command and control functions working effectively. Main drawbacks are network traffic and own network may be blocked.To reduce that confusion by clarifying terms and providing simple figures to measure comparisons between of cloud and predictable Computing, and identifying the top technical and non-technical obstacles and opportunities of Cloud Computing. The main concept used in Business continuity and service availability. The main drawbacks are very slow in connectivity, difficult to maintain as software reliability; to provide simple formulas to quantify comparisons between of cloud and conventional Computing, and identify the top technical and non-technical obstacles and opportunities of Cloud Computing. The main drawback is minimal management effort.

Server is accessed imitation terminals. The connection setup is limited. The main drawbacks are affected establishing host values; Risk and cost benefit issues and data leakages.Cloud providers and customers must share the responsibility for security and privacy in cloud computing environments, but sharing levels will differ for different delivery models, The main advantages are bounded false positive and false negative; it's also efficient and effective, SPOT by monitoring outgoing messages, simple and powerful Statistical tool. The main drawbacks are Time and Space complexity.In this paper we focus on the detection of the compromised machines in a network that are used for sending spam messages, which are commonly referred to as spam zombies.The disadvantages are Time and Space complexity.

Tointroduce a passive network monitoring system called BotHunter, It is a security threat and command control channel, communication to be engaged. It is potential of transfer and circulation attack and efficiency and effective. The main concept is Characteristics of compromised Machines in BotSniffer. The drawbacks are very long time to response the delay and network traffic.To describe attack graph generation algorithm and intrusion detection and results of attack graph analysis and to be execute in related work and future work. Main concept is NuSMV and Binary Decision Diagrams. The main drawback is worst case probability.The model used to analysis and be able to automatically integrate formal defenselessness specifications. The analysis must be able to scale to networks with thousands of machines. A defenselessness analysis tool can be useful to such a system administrator; the concept is Assumption of graph analysis. To reduce complexity functions. The main drawback is the order of attacks does not modified.MulVAL comprises a scanner and an analyzer, run on one host whenever new information arrives from the scanners. MulVAL models network configurations as abstract host access-control lists (HACL). This information can be provided by a firewall management tool such as the Smart Firewall. The concept is model and analyze network system. The drawbacks are use only small number of programs and complicated to arrange the components.

PROPOSED WORK

NICE utilize a new attack graph approach for attack uncovering and prevention by comparing attack activities and also propose important countermeasures. NICE optimizes the implementation on cloud servers to reduce reserve operation. Our study shows that NICE get through less calculate operating cost compared to alternative-based network intrusion uncovering solutions. We propose Network Intrusion detection and Countermeasure selection in virtual network systems (NICE) to establish a protection-in-strength intrusion detection framework. For better attack detection, NICE includes attack graph logical procedures into the intrusion detection methods. We must note that the design of NICE does not mean to improve any of the existing intrusion detection algorithms; definitely, NICE employs a reconfigurable effective networking approach to sense and answer the efforts to compromise VMs, thus preventing zombie VMs.



CONCLUSION

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. 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.NICE protocol to detect and mitigate collaborative attacks in the cloud virtual networking environment. NICE utilizes the attack graph model to conduct attack detection and prediction.

REFERENCES

[1] Coud Security 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] 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.

[8] G. Gu, J. Zhang, and W. Lee, “BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic,” Proc. 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. Security and Privacy, pp. 273-284, 2002,

[10] “NuSMV: A New Symbolic Model Checker,” http://afrodite.itc. it:1024/nusmv. Aug. 2012.