ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 9 September, 2014 Page No. 8071-8074

Analyze & Classify Intrusions to Detect Selective Measures to Optimize Intrusions in Virtual Network

K. Naveen Kumar[1], Madan Pojala[2] , P.Venkateswarlu Reddy[3]
M. Tech Student in CS [1], M. Tech Student in CS [2], Assistant Professor, CSE Department[3]
Sree Vidyanikethan Engineering College(Autonomous),[1], Sree Vidyanikethan Engineering College(Autonomous)[2] , Sree Vidyanikethan Engineering College(Autonomous)[3],Tirupathi, chittoor, Andhra pradesh, India.
[1]naveen28cse@gmail.com
[2]madan.0564@gmail.com
[3]venkateswarlucse@gmail.com

Abstract— Cloud computing provides a rich set of features and facilitate user to install softwares and applications in virtual machine (VM) temporally to finish their task with that software which is required and not available in cloud. But some attackers mislead this feature to introduce vulnerability as applications into VM. These applications are distributed over the virtual network and denial some services running over the VM accessing unknowingly by multiple users. To prevent vulnerabilities in VM we are introducing a network agent periodically scans the VM for vulnerable things and reported to attack analyse. It build attack graph by analyse the attack to know its type and apply selective measures to optimize it by network controller with help of VM Profiler.

Keywords— Cloud Computing, Intruders, Virtual machine, Vulnerability.

I. INTRODUCTION

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS), so we use that term. The datacenter hardware and software is what we will call a Cloud [1]. To understand the various applications of cloud computing it is essential to be aware of the types of cloud computing available. Cloud computing is broadly classified into public cloud, hybrid cloud, private cloud and community cloud. The different types of services provided by cloud computing are Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Storage as a Service (STaaS), Data as a service (DaaS), Business process as a Service (BPaaS), Test environment as a service (TEaaS), Desktop as a service (DaaS) and API as a service (APIaaS) [2].

The success of cloud computing lies in how much the data stored in cloud is kept secured against the hackers. Seven security issues by Gartner which cloud clients should advert are privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability [3].

The vital attack to be prevented is Distributed Denial of Service (DDOS) attacks in cloud computing environment. This type of attacks is often the source of cloud services disruptions. One of the efficient methods for detecting DDOS is to use the Intrusion Detection Systems (IDS), in order to assure usable cloud computing services [4].

DDOS attacks usually involve early stage actions such as multistep 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 multiphase 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 [5].

The DDOS attacks though are detected and the countermeasures are taken against it, they are high in NICE. The DDOS attacks are reduced very much in MDIDS thus

reducing the utilization of CPU, less time consumption for creating required virtual machine and the infrastructure response time is also reduced. The paper is organized as follows. Related work examines carefully the preceded researches in identifying the security threats against cloud and the counter measures taken. Related work is succeeded by NICE – Existing Approach. The next section is MDIDS – Proposed Approach. The Performance improvement in Cloud section discusses the advantages obtained by MDIDS over NICE. The conclusion and future work section consolidates the results obtained in this paper and the future research work that could be carried out having this paper as base.

II. Related Work

The DDOS is applied at different layers of OSI with increasing complexity and detection mechanism. The application layer DDOS is the more sophisticated form of threat which attacker can perform when the simple net – DDOS fails attacker shifts their distasteful strategies to application layer. Attacker runs the massive number of queries through victims' search engine to bring server down. The next layer of attack is session layer attack which includes DNS and SSL attacks which jams the session. The most traditional type of attack is network layer attack which is ICMP flooding, UDP flooding, SYN flooding. The DDOS in overall packs the server, bandwidth and resources [6].

The main problem faced in a cloud environment is the DDOS. During such a DDOS attack all consumers will get affected at the same time and will not be able to access the resources on the cloud. All client users send their request in the form of XML messages and they generally make use of the HTTP protocol. So the threat coming from distributed attacks are more and easy to implement by the attacker, but such attacks are generally difficult to detect and resolve by the administrator. So to resolve these attacks a specific approach for providing security based on various filters introduced. Five different filters which are used to detect and resolve XML and HTTP DDOS attack. This allows the security expert to detect the attack before it occurs and block or remove the suspicious client [7].

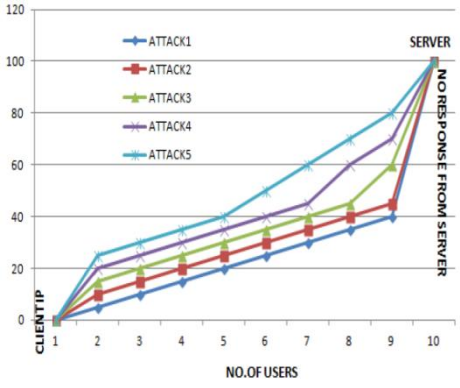
Grid and Cloud Computing Intrusion Detection System (GCCIDS) detects encrypted node communication and find the hidden attack trial which inspects and detects those attacks that network based and host based can't identify. It incorporates Knowledge and behavior analysis to identify specific intrusions. Signature based IDS monitor the packets in the network and identifies those threats by matching with database but It fails to detect those attacks that are not included in database. Signature based IDS will perform poor capturing in large volume of anomalies. Another problem is that Cloud Service Provider (CSP) hides the attack that is caused by intruder, due to distributed nature; cloud environment has high possibility for vulnerable resources. By impersonating legitimate users, the intruders can use a service's abundant resources maliciously. In Proposed System we combine few concepts which are available with new intrusion detection techniques. Here to merge Entropy based System with Anomaly detection System for providing multilevel Distributed Denial of Service (DDOS). This is done in two steps: First, Users are allowed to pass through router in network site in that it incorporates Detection Algorithm and detects for legitimate user. Second, again it pass through router placed in cloud site in that it incorporates confirmation Algorithm and checks for threshold value, if it 's beyond the threshold value it considered as legitimate user, else it's an intruder found in environment. This System is represented and maintained by as third party. When attack happens in environment, it sends notification message for client and advisory report to Cloud Service Provider (CSP) [8].

NICE, is to detect and mitigate collaborative attacks in the cloud virtual networking environment. NICE utilizes the attack graph model to conduct attack detection and prediction. It 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 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 [5].

MDIDS a proposed approach optimizes the implementation on cloud servers to minimize resource consumption. MDIDS includes two main phases, deploy a lightweight mirroring based network intrusion detection agent (MDIDS-A) and Deep Packet Inspection (DPI) is applied and virtual network reconfigurations can be deployed to the inspecting Virtual Machine (VM) to make the potential attack behaviors prominent.

III. Previous System

In a cloud system shared infrastructure benefits attackers to exploit vulnerabilities. The Distributed Denial of Service attacks have been counter-measured by approaches such as Entropy variation Method and Puzzle based Game theoretic Strategy. The efficiency of the existing methods may become reduced, when the attacks use more amounts of requests at a time.



The above Fig.1 illustrates the fact that there is almost six attacks which are all DDOS attacks occurs with number of users plotted against the time duration of the usage of the system by the users measured in milliseconds. As a result of these attacks, even though the clients expects and waits for the response from the cloud server the server does not register its response to the clients according to their requests. This increases the infra structure response time.

When the infra structure response time increases, it automatically increases the resource utilization. i.e. CPU utilization and also time taken to create a virtual machine.

IV. Proposed System

MDIDS incorporates a software switching solution to quarantine and inspect suspicious VMs for further investigation and protection. MDIDS employs a novel attack graph approach for attack detection and prevention by correlating attack behavior and also suggests effective counter measures. MDIDS is used to identify the source or target of the intrusion to detect multistep attack. It utilizes the attack graph model to conduct attack detection and prediction. It also establishes a defense-in-depth intrusion detection framework for detect mitigate DDOS attack in cloud environment. The DDOS attacks are prevented in MDIDS.

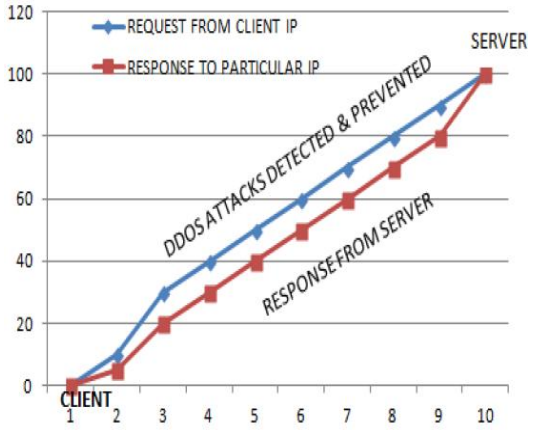


Fig. 2 Prevention of DDOS attacks using MDIDS

In the above Fig.2 there are no DDOS attacks. Though the number of users and the duration of usage of systems by the users are same as in NICE, the DDOS attack is prevented from happening in MDIDS. The response from the cloud server to the awaiting clients after their requests to the server is promptly delivered. The DDOS is detected and prevented early before intruding into the Cloud and causing damages to the system. MDIDS consumes less computational overhead compared to proxy-based network intrusion detection solutions. The infrastructure response time, CPU utilization and the time required to create a virtual machine are reduced when compared to NICE.

VI. Performance Improvement in Cloud

The amount of CPU utilized by MDIDS is less when compared to other intrusion detection system. The graph below highlights this fact.

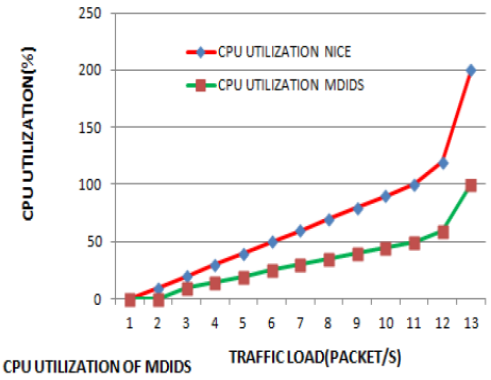


Fig. 3 CPU Utilization in MDIDS

The CPU utilization in mirror based MDIDS, proxy based MDIDS and MDIDS are compared. The CPU utilization is very low in MDIDS than in other two intrusion detection system. The CPU utilization is given in percentage against traffic load measured in packets per second. Proxy based MDIDS utilizes twice the amount of CPU than MDIDS for a traffic load of 15 packets per second. Mirror based MDID utilizes 35% more CPU than MDIDS for an equal traffic load. The IRT is analyzed in two phases. The IRT is calculated with the number of applications plotted against its response time measured in milliseconds. In the first phase IRT is calculated without the introduction of MDIDS in cloud.

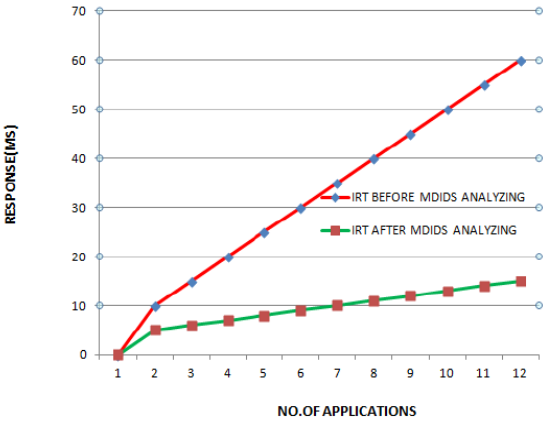


Fig. 4 Infra-structure Response Time Calculation

The IRT is very high before introducing MDIDS. The IRT becomes very low after the introduction of MDIDS. This clearly indicates that there is growth in the performance of cloud in MDIDS.

The service to the clients is implemented fastly in MDIDS. The time taken to create a required VM before detecting DDOS using MDIDS is more. The time in milliseconds and the number of VM created are noted and plotted. Before analyzing the DDOS , the VM creation taking 100milliseconds after detecting the DDOS using MDIDS the VM creation taking only 10milli-seconds.

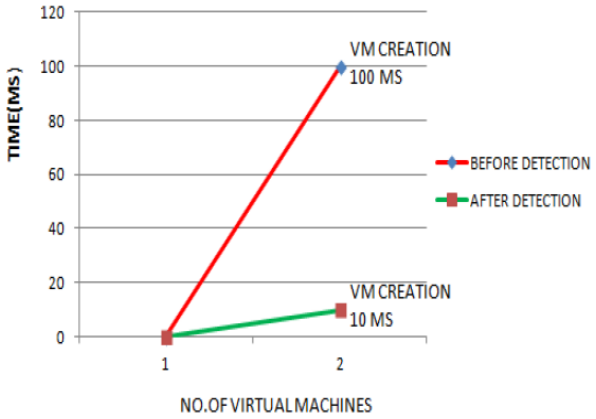


Fig. 5 Time Taken to Create Virtual Machine

The time taken to create one VM before detection is ten times the time taken to create it after detection.

VII. Conclusion and Future Work

MDIDS unlike NICE detects DDOS early and prevents the system from its attack. As a result there is an improvement in the performance of the cloud with the depletion in the CPU utilization, IRT and VM creation time. The future research can be done on investigating the scalability of the proposed MDIDS solution by investigating the decentralized network control and attack analysis model based on current study.

REFERENCES:

[1] Cloud Security Alliances,2010"Top Threats to Cloud Computing v1.0.
[2] Armbrust.M, Fox.A, Griffith.R, Joseph.A.D, Katz.R, Konwinski.A, Lee.G, Patterns.D,2010"A View of Cloud Computing," ACIM Comm., vol.53,no.4,pp.50-58.
[3] B.Joshi, A.Vijayan, and B.Joshi,2012"Securing Cloud Computing Environment against DDOS Attacks,"Proc.IEEE Int'f Conf Computer Comm. And Informatics(ICCCI'12).
[4] H.Takabi, J.B.Joshi,and G.Ahn,2010"Security and privacy Challenges in Cloud Computing Environment," IEEE Security and Privacy, Vol.8, no.6,pp.24-31.
[5] "Open vSwitch Project," May 2012.
[6] Z.Duan, P.Chen, F.Sanchez, Y.Dong, M.Stephenson,and J.Barker,2010"Detecting Spam Zombies by Monitoring Outgoing Messages,"IEEE Trans,Dependable and Secure Computing, vol.9, no.2,pp.198-210.
[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).
[8] G.Gu, J.Zhang, and W.Lee,2008"Botsniffer:Detecting Botnet Command and Control Channels in Network Traffic,"Proc.15th Ann.Network and Distributed System security Symp.(NDSS'08).
[9] O.Sheyner, J.Haines, S.Jha, R.Lippmann, and J.M.Wing,2010"Automated Generation and Distributed Symp.(NDSS'08).
[10] "NuSMV:A New Symbolic Model Checker,/nusmv.Aug 2012.
[11] O.Database,"Open Source Vulnerability Database(OVSDB)," 2012.
[12] A.Roy, D.S Kim, and K. Trivedi,2012" Scalable optimal Countermeasure Selection Using Implicit Enumeration on Attack countermeasure Trees," Proc.IEEE Int'I Conf.Dependable Systems Networks(DSN'12).
[13] N.Poolsappasit, R.Dewri, and I.Ray,2012"Dynamic Security Risk Management Using Bayesian Attack Graphs," IEEE Trans.,Dependable and secure computing, vol.9,no.1,pp.61-74.
[14] National Institute of standards and Technology,"National Vulnerability Database, NVD," 2012
[15]"Metasploit,2012..