Volume 5, Issue 9, September 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Smart Agent Based Security for VM in Cloud

Dr. K. Venkataramana

Department of Computer Science & Applications, KMM Institute of Post Graduate Studies,
Tirupati, Andhra Pradesh, India

Abstract— Cloud computing provides scope of using information technology resources and services in effective manner, but at same time it opens many uncertainties on security provisioning. Among these are the problem of securing the virtual-machine images that encapsulate each application of the cloud. Base of Cloud heavily relies on virtualization through which IaaS is provided on which PaaS and SaaS are supported to users. Virtual Machine (VM) which is similar to a physical machine, faces the same threats as that of physical machine like VM Attacks, VM Escape, and Denial of Service Attacks etc. VM image when deployed and exposed to network, it may be target of cyber-attacks and intrusions such as viruses, malwares, Trojan horses etc. So in this paper we have proposed agent based VM protection model, in which an SMART AGENT process or a thread does not allow the attacks like malwares, other malicious and unwanted software or program to run on the virtual environment of a cloud by comparing the features of the applications that are ready to run on VM with the built-in application features stored in the repository of SAE maintained securely in VMs.

Keywords— Cloud Computing-Security-Virtualization-Smart Agent--Malwares-VMSecurity

I. INTRODUCTION

The latest buzz word in IT sector is Cloud Computing which being endorsed as a low cost business model comprising of services at Infrastructure level, Platform level or Application level and delivered as public, private and hybrid models to users. In spite of providing lucrative benefits, as the Cloud runs on open Internet model which has become targets for attackers which leads to loss of information or disruption of services. As a result, ensuring security of the cloud is seen as a major Engineering challenge [1].

Cloud computing is TCP/IP based high development and integrations of computer technologies such as fast microprocessor, huge memory, high-speed network and reliable system architecture. Cloud computing, is a new paradigm of distributed computing, introduces many new ideas, concepts, technologies and architectural styles into enterprise service-oriented computing. A cloud may be thought of as a large pool of resources unified through virtualization or job scheduling techniques, these resources can be managed to dynamically scale up to match the load, using pay-per-resources business model. Cloud computing promotes a model for providing IT capacities over the Internet as services and on a lease based and on-demand style. A collection of technologies underpins the new computing paradigm, including Web Services, Virtualization, Utility Computing, and so on.

Cloud computing is typically described with a three layer stack, with each layer providing its own services, as illustrated in Fig-1. The Cloud Infrastructure Service or the Infrastructure as a Service (IaaS) provides IT infrastructures as a service over computer networks. The Cloud Platform Service or the Platform as a Service (PaaS) delivers computing platforms as a service to sustain the cloud applications. The Cloud Application Services or Software as a Service (SaaS) delivers software as a service over the network, allowing users to use applications without having to install and run software on their own computers. This document is a template. An electronic copy can be downloaded from the Journal website. For questions on paper guidelines, please contact the journal publications committee as indicated on the journal website. Information about final paper submission is available from the conference website.

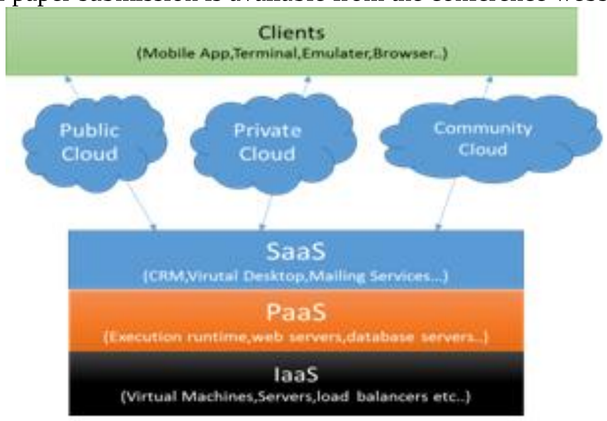
Clients
(Mobile App,Terminal,Emulater,Browser..)
Public Cloud
Private Cloud
Community Cloud
SaaS
(CRM,Virutal Desktop,Mailing Services...)
PaaS
(Execution runtime,web servers,database servers..)
IaaS
(Virtual Machines,Servers,load balancers etc..)

Fig:-1 Cloud Layers and Deployment Models

Cloud deployment models include public, private, community, and hybrid clouds. Public clouds are external or publicly available cloud environments that are accessible to multiple tenants, whereas private clouds are typically tailored environments with dedicated virtualized resources for particular organizations. Similarly, community clouds are tailored for particular groups of customers. In order to improve their business and profits after recession IT companies, many organizations rely on heterogeneous applications developed with open sources which uses web services hosted on a set of clustered database servers which pays as per their usage [2]. At the other end to accommodate this, organizations would consider ways to reduce computing power, electricity charges, space costs in datacentres, also supports green computing etc. To achieve above the most efficient solutions is virtualization. Virtualization is a technology that combines, or divides computing resources to present one or a number of functional environments. This is achieved through techniques such as hardware or software partitioning or assemblage, time-sharing and other methods. Each virtual machine was the representation of a physical machine; making the users believe that they were accessing the physical system directly. It enabled time-sharing and resource sharing on very expensive hardware. To the end-user this was completely transparent [3].

The virtualization concept is better explained in figure-2 where the hypervisor software will virtualize layers like Memory, CPU, and Storage etc. which allows to create Virtual machines for each client or as the requirement demands it to do so. Even though virtualization will provide full utilization of resources at the same time the problem of security arises.

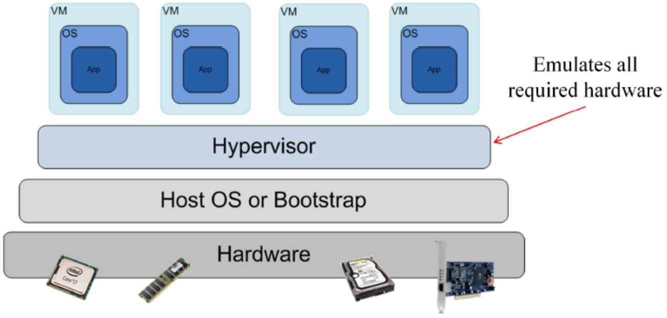

Fig:-2 Virtualization

The attacks or security threats that work in a physical world also work in a virtualized world and in fact could be more devastating because they could propagate much more rapidly within a virtualized environment, where all virtual instances are within the same physical host. This means that if a host server is attacked and the virtualization layer is compromised, it can expose all the [virtual machines (VMs)] in the infrastructure and compromise all hosted applications and data. So in this paper we have proposed model based on Agent services which will protect VM from attacks and could minimize security flaws.

II. LITERATURE SURVEY

In the paper by Andre van Cleeff et.al [4], has studied about implications of virtualization on security which states introspection of VM leads to security problem as there is possibility of attack by another, Identification problem when VM is copied with same configuration, spreading of infections to other VMs when copied or moved.

In the paper by Andrew R. Riddle and Soon M. Chung, discussed [5] about how cloud computing security is compromised due to hypervisor. The malicious VM running on hypervisor may cause denial of service attack to steal resources and slow down the other co-resident VMs using a side-channel. A side-channel typically makes use of shared resources, such as the CPU cache, memory, network, power consumption, etc. to extract information.

In the paper[6] by Hsin-Yi Tsai et.al, we can find how VM Hoping ,VM Diversity, VM Mobility, VM Denial of Service will cause problems related to Confidentiality, Availability, Integrity in SaaS, PaaS and IaaS service layers. Attack severity ranges from leaking sensitive information to completely compromising the guest OS. Also, because VM mobility offers increased flexibility, it similarly increases the complexity of security management.

In the SADE system proposed by Matthew Conover et.al [7], where an agent is injected into VM to scan the signatures in memory to detect whether it is an valid or invalid process to enhance security. In this model virtual appliance VM performs on behalf of user VMs such as injection agent code or to execute trusted code in VM. If the channel of injection is known to malicious VM then it is easy to inject virus code into other VMs which leads to attacks as we already discussed. Cryptographic techniques is applied to protect data and to provide security which may not be applied to cloud computing in all aspects, since keys which are to be secured may be compromised due to dishonest infrastructure providers. Such providers have full control of the cloud infrastructure. They can configure and modify the cloud infrastructure to allow unrestricted access to a malicious hypervisor module, install malicious hardware, perform a side channel attack, and modify system software to get access to the customer’s data [8]. So in this paper we have proposed an agent based model which detects an unauthorized process or malware or virus and kills the process or report it to administer for further action.

III. MALWARES

In this section we discuss about code malicious programs or otherwise malwares that leads to security breach in any computing or in virtual environments. Malware is a malicious software, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behaviour. Malware may be Computer viruses & Worms, Trojan horses, Spyware, Dishonest adware [9].

Virus is a computer program usually hidden within another seemingly innocuous program that produces copies of itself and inserts them into other programs or files, and that usually performs a malicious action. A computer worm is a self-replicating malware computer program, which uses a computer network to send copies of itself to other nodes or VM's and it may do so without any user intervention. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even by consuming bandwidth, whereas viruses almost always corrupt or modify files on a target VM's or data centres in cloud.

A Trojan horse, or Trojan, is a destructive program that masquerades as an application. The software initially appears to perform a desirable function for the user prior to installation and/or execution, but steals information or harms the system. Unlike viruses or worms, Trojan horses do not replicate themselves, but they can be just as destructive. Spyware is a type of malware that can be installed on computers, and which collects small pieces of information about users without their knowledge. The presence of spyware is typically hidden from the user, and can be difficult to detect. Spyware will send information from one application from on VM to another VM which leads to breach of SLA or VM Security. A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications. These type of malwares when present in root VM may hamper the operations of other VM's under its control.

Other type of Malware, a Data-stealing malware is a web threat that divest victims of personal and proprietary information with the intent of monetizing stolen data through direct use or underground distribution. These malicious process have the following characteristics [10] which should be analysed to avoid attacks from within the VM or from outside the VM. VM's security will be in threat due to following reasons such as

Does not leave traces of the event

- The malware is typically stored in a cache that is routinely flushed
- The malware may be installed via a drive-by-download process
- The website hosting the malware as well as the malware is generally temporary or rogue

Frequently changes and extends its functions

- It is difficult for antivirus software to detect final payload attributes due to the combination(s) of malware components
- The malware uses multiple file encryption levels.

Thwarts Intrusion Detection Systems (IDS) after successful installation

- There are no perceivable network anomalies
- The malware hides in web traffic in applications in SaaS
- The malware is stealthier in terms of traffic and resource use

Thwarts disk encryption

- Data is stolen during decryption and display
- The malware can record keystrokes, passwords, and screenshots
- Thwarts Data Loss Prevention (DLP)
- Leakage protection hinges on metadata tagging, not everything is tagged
- Miscreants can use encryption to port data

By considering above facts VM should be secured by above malwares in order to improve cloud virtual environment security.

IV. SMART AGENT VM SECURITY MODEL

The proposed model is based on Agent based architecture in which software agents will verify and allow process to execute in Virtual machine. In this model we create a Smart agent which will learn to find malwares, virus programs, programs which are using resources more than required and avoids its execution. A smart agent (or simply an agent) is a program that gathers information and updates virus or malware definitions without your immediate presence and on some regular schedule. Smart agent program, using parameters you have provided, searches entire Child Partition VM gathers information in, and presents it to SAE (Smart Agent Environment) shown in Figure in periodic basis.

Smart Agent Environment (SAE) is installed in each of VM Contains following Components which provides SA to provide the proposed security to VM. SAE is different at Root Partition which has ability to create SA at child partitions when VM starts in Child Partition. SA is created by Smart Agent Creator SAC which is an authenticated process created by Root partition. SA will run as DAEMON process in VM's in child partitions to protect from unauthorized process.

SA – Smart Agent is a DAEMON process which created by SAE at root partition and executed at each of child partition which collects information of all the unauthorized process at child partition VM's and updates SAE and improves security of VM.

MPR – Malware Process Repository which stores or will be updated by Smart Agent (SA) when new definitions are found.

MPC- Malware Process Comparator which verifies the process properties with MPR which when matches blocks the Process execution by notifying it with VMWP or VSC through VMBus in Hyper-V architecture shown in figure-3.

ACR-Application Configuration Repository which stores properties or configuration of Process in an application that is said to be executed on VM.

ACV-Application Configuration Verifier which verifies every process characteristics like memory usage, device usage and reports to VSC or VMWP through VMBus to kill the process. ACV uses machine learning techniques to come to conclusion if process in valid or invalid/unauthorized.

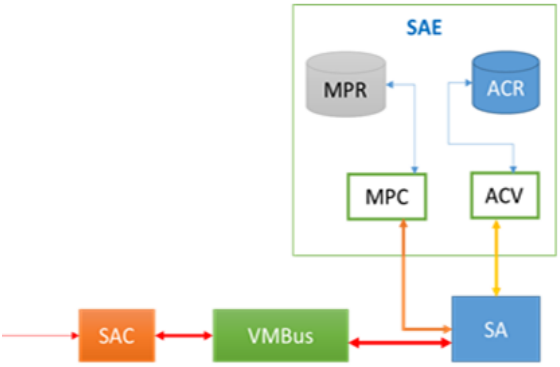

Fig-3 Smart Agent Environment with Smart Agent

A. *Working of Smart Agent*

The proposed Smart Agent model is designed based on Hyper-V Architecture of Microsoft Virtualization mechanism [12]. In Hyper-V model Root Partition creates child partitions on which Guest operating systems are install and uses virtualization services of underlying architecture of machine with help of Hypervisor. In this model Smart Agent Environment (SAE) is installed in Root Partition as well as at the Child partitions when it is created, components of SAE is shown in figure-4. At Root Partition SAE contains Smart Agent Creator Process (SAC) which will create SA in every child partition every time when VM is starting or guest OS is started as to make SA unaffected by user process at Guest OS. SAE at Child partitions cannot create SA on their own but allows SA running in its VM to verify and update repositories in it.

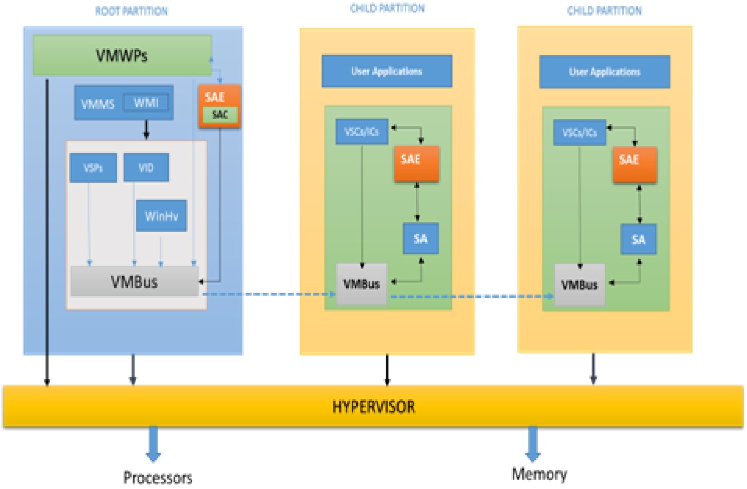

Fig-4 Smart Agent Based Hyper-V Architecture

Smart Agent is an software process which runs periodically at background check every process running in user applications running in Child partitions and sends signals to VSC's or ICs through VMBus which in turn send alerts to VMWPs or VMMS in root partition so as to take necessary action to terminate the process or closes the VM which will harm other VM's. SA will allow process created in that VM which run in limits in terms of resource usage and protects VM by attacker. Smart agent updates the SAE repositories to make SAE efficient enough to terminate unauthorized Malware or user process in future. Smart Agent can also be used to make decision in terms of continuation of process in user application or not to avoid memory crash or in case of load balancing by collecting process data in VM.

V. SECURITY ANALYSIS

The proposed Smart agent based security model will protect Virtual machine from various threats like VMHoping [12], VMMobility, VMDenial of Service or attacks from malware programs. Smart Agent (SA) will not allow attacker process to run in current VM to access VM's configuration thus avoids VMHoping. In case of VM mobility Smart VM Agent Environment is also mobilized with VM hence VM will be protected with SA created by SAE of Root Partition. As the SA verifies the resources used by process we can prevent DoS attacks using proper configurations. In case of process exceeding the limit SA will kill the process thus avoid VM Denial of Service threat.

VI. CONCLUSIONS

In this paper cloud computing and the use of virtualization in cloud computing to virtualize resources is discussed along with smart agent based security to protect VM from malware or unauthorized programs, which can access shared memory of other users virtual machines causing data leakage or security breach . The proposed model is based on Hyper-V architecture of Microsoft which can also extended to other architecture like VMWare etc.

REFERENCES

[1] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance: O'Reilly Media, Inc., 2009.

[2] M. Steinder, I. Whalley, D. Carrera, I. Gaweda, and D.Chess, “Server virtualization in autonomic management of heterogeneous workloads”, Integrated Network Management, IEEE, 2007, pp. 139-144.

[3] Amir Ali Semnanian, Jeffrey Pham et.al., “Virtualization Technology and its Impact on Computer Hardware Architecture”, 2011 Eighth International Conference on Information Technology: New Generations, IEEE, DOI 10.1109/ITNG.2011.127

[4] Andre van Cleeff, Wolter Pieters, Roel Wieringa, Security Implications of Virtualization: A Literature Study, 2009 International Conference on Computational Science and Engineering,IEEE

[5] Andrew R. Riddle and Soon M. Chung, A Survey on the Security of Hypervisors in Cloud Computing, 2015 IEEE 35th International Conference on Distributed Computing Systems Workshops

[6] Hsin-Yi Tsai,Melanie Siebenhaar and André Miede,Yu-Lun Huang,Ralf Steinmetz, Threat as a Service? Virtualization’s Impact on Cloud Security, IT Professinal, IEEE, 2012

[7] Tzi-cker Chiueh, Matthew Conover, Bruce Montague Surreptitious Deployment and Execution of Kernel Agents in Windows Guests, 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing

[8] F. Rocha and M. Correia, ”Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud”, Proc. 1st Intl. Workshop of Dependability of Clouds, Data Centers and Virtual Computing Environments, pp.1-6. 2011.

[9] https://en.wikipedia.org/wiki/Malware

[10] Internet Security , PediaPress

[11] Muragesansan, Intelligent software agents on the Internet and Web,TENCON '97. IEEE Region 10 Annual Conference. Speech and Image Technologies for Computing and Telecommunications. Proceedings of IEEE (Volume: 1)

[12] K. Owens, “Securing Virtual Computer Infrastructure in the Cloud,” white paper, Savvis Communications Corp., 2009