IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 3 Issue 7 July, 2015

A Survey on Secure Virtualization for Cloud Computing

Author: Eden Sequeira[1]; Karishma S. Kumar[2]

Affiliation: Research Scholar[1]; Research Schlor[2]

E-mail: edensequeira@gmail.com[1]; karishmakumar0505@gmail.com[2]

ABSTRACT

Today's one of the most exciting technologies is cloud computing, because it can reduce the cost and complexity of applications, and it is flexible and scalable. Cloud services are providing on-demand resources via virtualization technologies. Virtualization refers to the abstraction of computer resources. The purpose of virtual computing environment is to improve resource utilization by providing a unified integrated operating platform for users and applications. In this paper, we address different methods for the security of virtualization in cloud computing environment.

Keywords: Virtualization, hypervisor

1. INTRODUCTION

In recent years, cloud computing has emerged as one of the fastest-growing segments of the IT industry and more and more businesses have gone to the cloud. Cloud computing has been deployed in a variety of data storages and data centers, network communications, data managements. Cloud computing offers an effective way to reduce IT expenses, Capital Expenditure (CapEx), and Operational Expenditure (OpEx) and thus it offers economic benefits to users and organizations. cloud computing is defined as a pool of virtualized computer resources. Generally, Cloud providers use virtualization technologies combined with self-service abilities for computing resources via network infrastructures, especially the Internet and multiple virtual machines are hosted on the same physical server. Based on virtualization, the cloud computing paradigm allows workloads to be deployed and scaled-out quickly through the rapid provisioning of Virtual Machines or physical machines. A cloud computing platform supports redundant, self-recovering, highly scalable programming models that allow workloads to recover from many inevitable hardware/software failures. Therefore, in clouds, costumers only pay for what they use and do not pay for local resources, such as storage or infrastructure. A virtual appliance relieves some of the notable management issues because most of the maintenance, software updates, configuration and other management tasks are automated and centralized at the data center by the cloud provider responsible for them[1].

2. TYPES OF VIRTUALIZATION

There are two types of virtualization environments in which VMM is deployed. Type I is known as Full virtualization where VMM is interfacing directly with the system hardware this type of architecture is also called as native architecture, Figure 1. Type II is not interfacing directly with the hardware of the system, rather it runs as an application along side with the host OS. Type II is called Para-virtualization Figure 2.

2.1 Full Virtualization

Full virtualization is considered when the hypervisor is implemented directly on top of physical hardware or embedded in the host OS kernel. It is also called hardware virtualization because shared resources such as device drivers and hardware layer resources are virtualized by the VMM for guest OS. An example of this type is the Xen hypervisor, KVM hypervisor.

2.2 Para Virtualization

Para virtualization is commonly deployed on those machines that don't support Full virtualization such as Intel "x86" architecture. It runs as software and it is enabled by the host OS which provides I\O drivers and bootstrapping code[4, 7, 8]. This type is known to be less secure because no matter how secure the VMM is, it is effected by the security of

the host OS itself. An example of this virtualization architecture is the implementation of virtual environments using VMware, Sun VirtualBox, and Microsoft Virtual PC.

3. SECURITY VULNERABILITIES IN VIRTUALIZATION

Most of security threats identified in a virtual machine environment are very similar to the security threats associated with any physical system.

3.1 Attack between VMs or between VMs and VMM

Attack between VMs or between VMs and VMM Isolation is the primary benefit of virtualization. . This benefit, if not carefully deployed will become a threat to the environment. The inner-attack between VMs(virtual machine) or between VMs and VMM(virtual machine monitor) is caused due to poor isolation or inappropriate access control policy.

3.2 VM escape

Virtual machines are allowed to share the resources of the host machine but still can provide isolation between VMs and between the VMs and the host..VM escape is one of the software bug which happens if the isolation between the host and between the VMs is compromised. In the case of VM escape, the program running in a virtual machine is able to completely bypass the VMM layer, and get access to the host machine. Since the host machine is the root of security of a virtual system, the program which gain access to the host machine also gains the root privileges basically escapes from the virtual machine privileges.

3.3 Virtual Machine controlled by Host Machine

The control point of virtual environment is the host machine. Different virtualization technologies have different implications for the host machine to influence the VMs up running in the system.

- The host can start, shutdown, pause and restart the VMs.
- The host is able to monitor and modify the resources available for the virtual machines.
- The host if given enough rights can monitor the applications running inside the VMs.
- The host can view, copy, and likely to modify the data stored in the virtual disks assigned to the VMs.

3.4 Denial of Service

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.

4. VIRTUALIZATION SECURITY FRAMEWORK

Virtualization security framework is organized effectively in two modules which are virtual system security and virtualization security management.

The virtual system security consists of three layers: The fist layer is Physical Resource layer. The second layer is VMM which is the most important layer that facilitates with security mechanisms to protect VMs up running. The top layer is VMs that provide virtualization services to consumers. Virtualization security management protects the framework from attacks and threats[2].

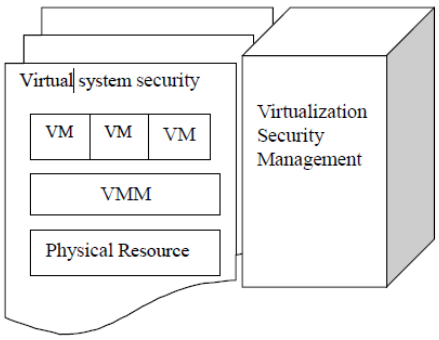

Fig 1: A Virtualization Security framework

4.1 Virtual system security

4.1.1 VM system architecture security

A secure VM system should be protected by a robust, efficient and flexible VM system architecture. The structure in figure has highest efficiency and flexibility.. But it is the more complex . In this architecture, security control is separated from the VMM layer so security control becomes an individual layer. Then security control for the VMM layer is transparent.

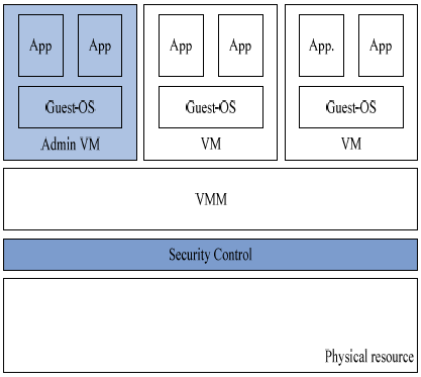

Fig 2: VM system architecture where security control is deplyed to protect VMM.

4.1.2 Access control

Access control in virtual environment refers to the practice of restricting entrance to a resource to authorized VM.

4.1.3 Virtual firewall

A Virtual Firewall(VF) is a firewall deployed and running entirely within a virtual environment and which provides the packet filtering and monitoring.

5. VIRTUALIZATION SECURITY ARCHITECTURE

"When the workload of the VM increases abnormally, the VM may be a victim or an attacker"

In this architecture HSEM and HREM are the main components of the security system, and all the other parts of the security system communicate with them, but HSEM decides if the VM is an attacker or a victim. VSEM and VREM consume low resources of the VM, but they help to secure VMs against attacks[3].

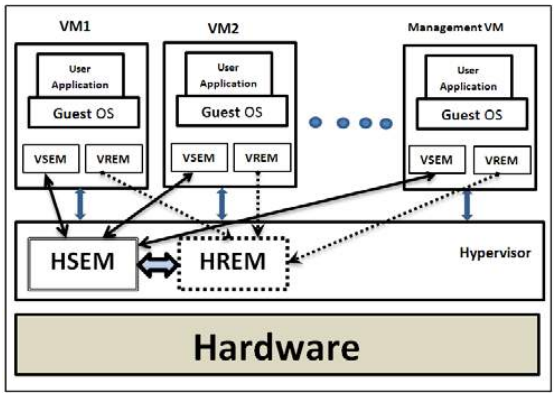

Fig 3: Architecture of secured virtualization

VSEM acts as sensors which is a two level controller and behaviour recorder in the cloud system that helps HSEM identify attacks and malicious behaviour with less processing. It also monitors security-related behaviours of VMs and reports them to HSEM. VSEMs have two levels of monitoring:

1) Level 1

In this level, the VSEMs monitor their own VMs. In this level VSEM collects of the source and destination addresses which are in head of data, number of unsuccessful and successful tries in sending data, and number of requests that were sent to the hypervisor.

2) Level 2

In this level, the VSEM monitors and captures the activity of the VM in more detail, such as VM's special request from the hypervisor, details of requested resources (e.g. the number of requests), and the destination transmitted packets (to recognize if it is in the same provider's environment or outside).

VREM monitors reliability-related parameters, such as workload, and notifies the load-balancer (within the hypervisor) about the parameter results. VREM is also used for security purposes.

6. HIERARCHICAL SECURE VIRTUALIZATION MODEL

The Hierarchical Secure Virtual Model (HSVM) uses standard cloud architecture (See Figure 1), which build IaaS on Virtual Machines (VMs) and workload are usually integrated from the guest OS and the user processes.

Virtualization takes place inside V-Basement, instead of having a solid virtualization. Hence virtualization could be classified based on services required by end guest machine (VM), regardless of who is going to use this machine as service user (SU). This will increase the feasibility of applying security procedures. It is necessary to specify IDS for each data flow source based on its application (e.g. Web Server, Data Storage, etc.). This specification allows for lightweight IDSs, instead of huge resource-consuming IDS[4].

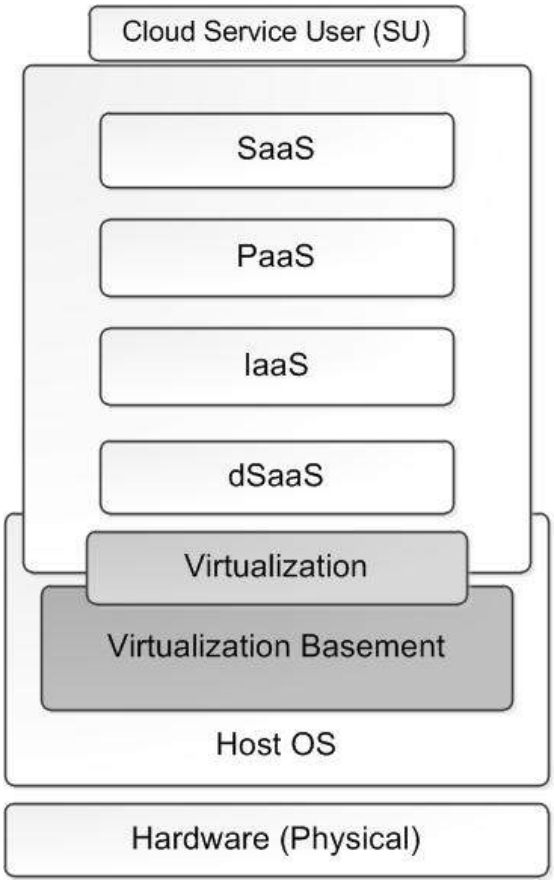

Fig 4: Hirachichal Secure Virtual Model for cloud Security

6.1 Primary Virtual Mechanism

Each PVM contains only specific group of services and applications at the end VMs. Also Inter-PVM Monitor module is added to enable secure communication between PVMs. V-Basement Communicator provides routines and interfaces for PVM to communicate with Host OS. the VM-Shadow has all required information to regenerate a shadow copy to the closest possible state of a selected VM on-demand.

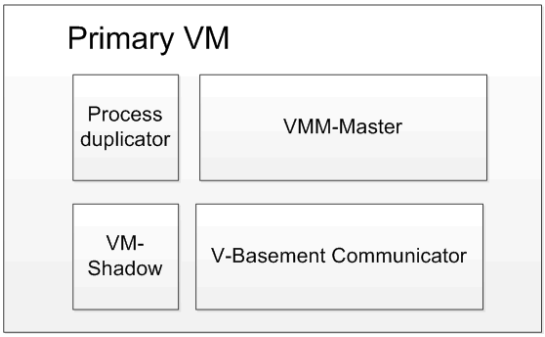

Fig 5: Primary VM-Master

6.2 Virtual Machine Monitor-Master

The VMM-Master coordinates all VMMs inside the primary VM.

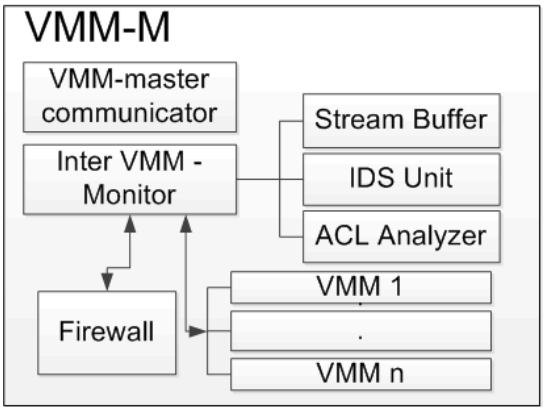

Fig 6: Virtual Machine Monitor-Master

6.3 Virtualization Basement (V-Basement)

V-Basement provides abstracted virtualization by dividing virtualization method hierarchically into primary VMs and the following modules. Inter-PVM Monitor performs VMM roles between PVMs, providing secure communication channels between all the above layers and the actual physical layer (hardware) through Host OS. It also has direct access to network layer.

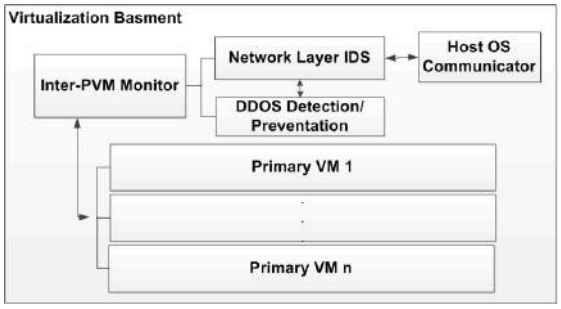

Fig 7: Vrtualization Basement

7. CONCLUSION

Virtualization security framework aim at the vulnerabilities. In this framework, VM system architecture can solve the problem of virtualization security effectively, and virtualization security management settles the question that various VM managements bring. try to reduce the workload, decentralize security-related tasks between hypervisor and VMs, and convert the centralized security system to a distributed one. HSVM proposes a novel hierarchical mechanism which

significantly improves vendor control in IaaS. In addition, it provides a practical solution by reacting to intrusions with an isolate-conquer approach.

8. REFERENCES

[1] G. J. Popek and R. P. Goldberg, "Formal requirements for virtualizable third generation architectures," Comm. ACM, vol. 17, no. 7, pp. 412–421.

[2] Shengmei Luo，Zhaoji Lin，Xiaohua Chen, "Virtualization security for cloud computing service", International Conference on Cloud and Service Computing, 2011.

[3] Farzad Sabahi, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology", International Journal of Machine Learning and Computing, Vol. 2, No. 1, February 2012.

[4] Sina Manavi, Sadra Mohammadalian, "Hierarchical Secure Virtualization Model for Cloud", Faculty of Computer Science and Information Technology Universiti Putra Malaysia, 43400 UPM Serdang, Selangor.