Term Paper 2

Secure Virtualization In Cloud Environment

Swapnil Hasabe
Computer Science
University of Texas at Dallas
sdh140430@utdallas.edu
CS6301: Securing and Developing Cloud
Instructor: Dr. Bhavani Thuraisingham

ABSTRACT:

Despite the large development in the field of cloud computing, security is still one of the major concerns to cloud computing. Most cloud services (e.g. Amazon EC2) are offered at low cost exchange of less security. For example, if user is allowed to access host disk files to take snapshot of whole system. In cloud computing, virtualization is considered as an important technique which delivers Infrastructure as a Service which separates data, application and network from hardware constraints. Also, cloud computing I defined as pool of virtual computers. In this paper, different approaches of securing cloud virtualization have been explored. Most of the current requirements involve virtual servers because virtual servers provide many benefits like scalability, cost saving, energy saving and resource savings. In this paper, different possible attacks on virtualization and their possible solutions have been discussed.

APPROACHES:

There are different approaches how they handle their virtual machine.
In each approach, how these virtualizations can be attacked is discussed.
1. **Operating System-Based Virtualization**: In this approach, attacker can have the control over all virtual machines by injecting controlling scripts into host operating system.
2. **Application-Based Virtualization**: Security issues of this approach are same as operating system- based virtualization.
3. **Hypervisor Based Virtualization**: In this model, hypervisor shares the system resources across the all virtual machines. This approach uses the Intrusion Detection System tool to ensure the security. But It is vulnerable to single point of failure. If the hypervisor fails or the attacker gains control over it, then all VMs are under the attacker's control.

Following are approaches of how to secure virtualizations:

1. **Hypervisor Security**: A hypervisor has its own security platform, and it has the capability to control everything within virtualization host. Hypervisor can be reason that all virtual machines get affected.

There are many security issues. One of them is when an attacker attacks the hypervisor and takes control of it. After that attacker will have the control over its resources.

a) Hypervisor has its own control over the hardware of the host machine. Also, it can access its resources. This ability of hypervisor provides security to infrastructure. Hypervisor can play of firewall as it resides between guest OS and host machine hardware. It prevents the all attacks to the infrastructure.

b) As mentioned before, Hypervisor is placed between the guest operating system and host machine hardware. So, even attack happens at guest OS, the hypervisor can detect it and can take appropriate action.

c) The IDSs can be used in hypervisor level, because all the transaction between the VMs and the hardware is under control. It is always better to have IDS in hypervisor.

2**. Farzad Sabahi proposed architecture of secured virtualization for cloud environment using Hypervisor-based technology.**

Architecture of Secured Virtualization:

HSEM and HREM are the main components of the security system, and all the other parts of the security system communicate with them. HSEM has following functions: i) it decides if the VM is an attacker or a victim. ii) HSEM receives behavioral information from VSEM and HREM iii) HSEM notifies the hypervisor about which VM is under Level-2 monitoring to get status.

Figure 3 illustrates the new secure architecture

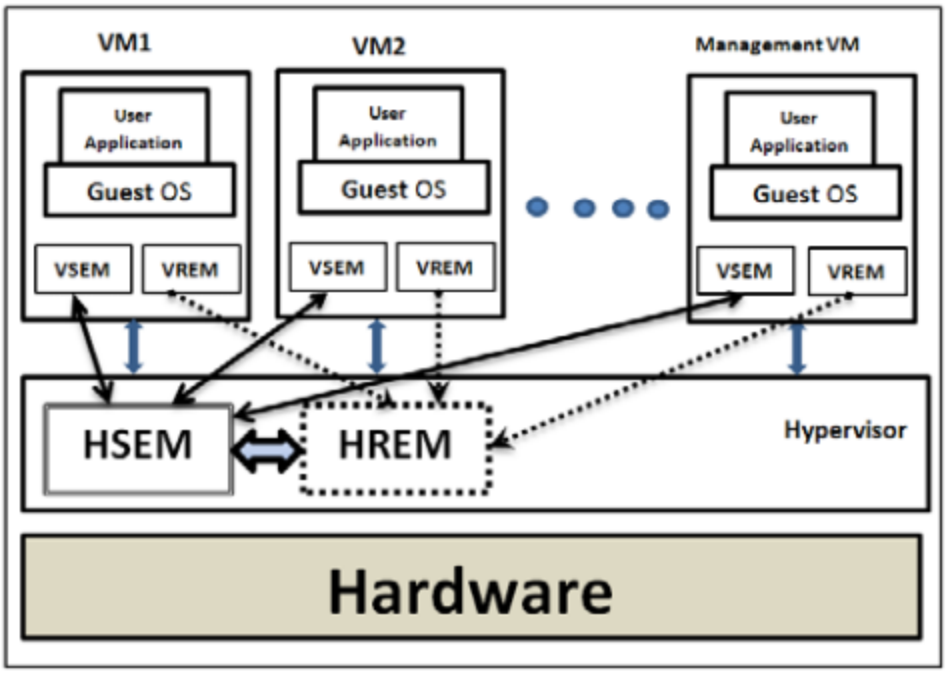
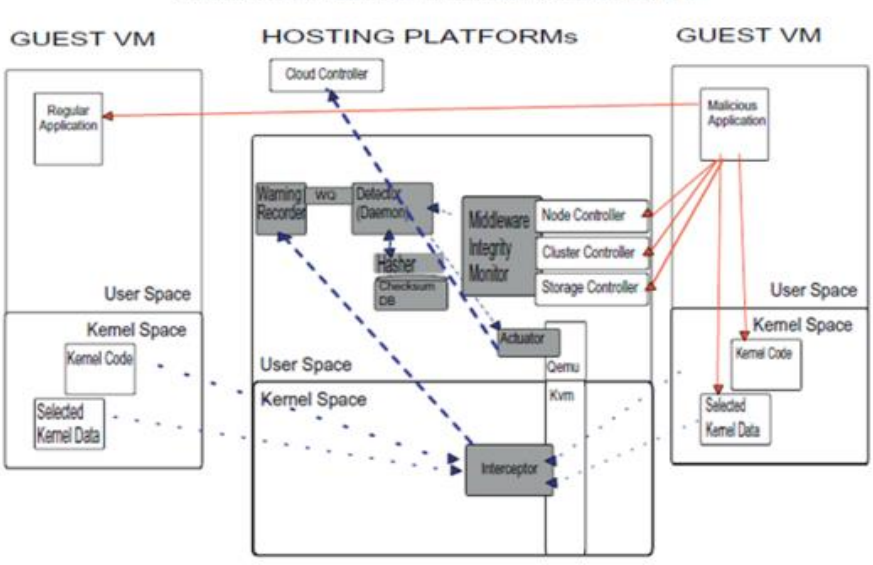


Fig. 3. Architecture of secured virtualization

3. **A Host-side Architecture for Securing Virtualization in Cloud Environment**:



Following are the modules which provide the security features to this architecture

Interceptor: This module takes care that attacker will not detect third party security. The interceptor does not block any traffic. Interceptor makes system intelligent. Also, it keeps an eye on all guest activities. It restores the module which gets affected by attacker.

Warning Recorder: It receives the analysis done by interceptor directly. It uses warning pool for security checks.

Evaluator and hasher: It also performs security checks based on the priorities of the warning pool and the warning recorder makes warning pool. Increased warning will lead to a security alert.

Actuator: The actuator actually makes the final decision whether to flag a security alert or not after receiving confirmation from Evaluator, hasher, and warning recorder.

ANALYSIS:

A Host Side Architecture for Secure Virtualization for cloud environment:

As this system is asynchronous in nature, it proves itself as CPU free. It reduces the complexity of behaviors on I/O operations. Warning recorder plays an important role of doing analysis in this architecture. File integrity check property makes it more secure. Modules are attached to key components of this system

Following are the best practices for securing virtualization and cloud:

1. Self- Defending Virtual Machine Security:

VM-level protection is very important in a virtualized or cloud computing environment. Enterprise can distribute application on same host .This ensures that enterprises will have the maximum the benefits of virtualization. VM level protection keeps all VMs secured so that all data get secured when it is travelling from private to public cloud.

2. **Layer coordinated Defenses:**

- These include security layers such as firewalls, intrusion detection and prevention; file integrity monitoring, log inspection, and anti-malware protection.
- A firewall reduces the attack surface of virtualized servers in cloud computing environments.
- It should contain centralized management of server firewall policy.
- Intrusion detection and prevention systems (IDS/IPS): Implementing IDS/IPS within the virtualized environment can prevent applications and operating systems from newly discovered vulnerabilities. It also gives timely protection against known and zero day attacks.

- File integrity monitoring is used to detect the malicious behavior which also gives alarm that virtual cloud environment is compromised.
- Log inspection captures all the events in log files. It also considers the risk factors of all attacks it knows and gives priority in the log.
- Anti-malware protection defends against viruses, spyware, Trojans and other malware.

3. **Security Optimized for Virtual cloud environment**:
   - It ensures other guest VMs are secured.
   - Enhances virtual server performance by running full system scans from the separate scanning VM.
   - It provides web application protection, application control, firewall, anti- malware.
4. **Visibility, Auditing, Reporting**
5. **Encryption for virtual and cloud environment**:
   - Provide end to end encryption between communicating party
   - Policy based key management
   - Identity and integration based validation
   - Separation between business and cloud service provider
6. **Security that travel with data**
   - It ensures that whenever data is travelling from private cloud to public cloud, it must be always secured.

CONCLUSION:

1. In this paper, host side novel architecture design is been discussed. It satisfies the main objective of securing virtualization on cloud environments. The architecture is purely host-integrated and remains transparent to the guest VMs. Architecture make the system more intelligent so that attacker would need many years to find only faults in the system. Making damage of system is even more difficult.

2. This paper includes security best practices which address the security against threats and issues relevant to virtualization and cloud environment.

3. In the hypervisor based architecture, workload is reduced and decentralization of security related task between VM and hypervisor. It converts its centralized security system to distributed one.

References:

1. G. Texiwill, Is Network Security the Major Component of Virtualization Security?, 2009.

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

3. http://resources.infosecinstitute.com/virtualization-security-cloud-computing/

4. Lombardi F, Di Pietro R – Secure virtualization for cloud computing, 2010

5.
http://www.websense.com/content/support/library/web/hosted/admin_guide/ldap_directories.aspx

6. T. Ristenpart and e. al, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," presented at the 16th ACM conference on Computer and communications security,Chicago, IL, November 9-13, 2009.

7. "Securing Virtualization in Real-World Environments," White paper, 2009.

8. F. Sabahi, "Intrusion Detection Techniques performance in Cloud Environments " in Proc. Conf. on Computer Design and Engineering, Kuala Lumpur, Malaysia, 2011, pp. 398-402.

9. P. Sefton, "Privacy and data control in the era of cloud computing."

10. Software Engineering Institute reports, N. Mead, E. Hough, and T. Sehny, "Security quality requirements engineering (SQUARE) methodolgy," Carnegie Mellon Software Engineering Institute, 2005.

11.R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masouka, and J. Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," presented at the ACM Cloud Computing Security Workshop, Chicago, Illinois, USA., 2009.

12. http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/rpt_security-best practices.pdf