ASecLmVm: Approaches to Secure Live Migration of Virtual Machine

Prabhat Pandey[1] , Prof. Jyoti sondhi[2], Prof. Anurag Shrivastava[3]

[1]PG Scholar , [2]Assistant Professor, [3] Associate Professor & HOD, Department of CSE, NRIIRT, Bhopal – 462022, India

Abstract- Cloud computing is emerging as the next generation platform which would facilitate the user to pay as you use mode as per requirement. The primary aim of Cloud Computing is to provide efficient access to remote and geographically distributed resources with the help of Virtualization in Infrastructure as a Service (IaaS). We need a different kind of virtual machines (VM) as per the requirement and cloud provider provides these services as per the Service Level Agreement (SLA) to ensure QoS. Virtual machine monitor (VMM) virtualizes the machine's resources in terms of CPU, memory, storage, network and I/O devices to allow multiple operating systems running in different VMs to operate and access the network concurrently. A key feature of virtualization is live migration (LM) that allows the transfer of virtual machine from one physical server to another without interrupting the services running in virtual machine. However, live migration is still in an early stage of implementation and its security is yet to be evaluated. The security concern of live migration is a major factor for its adoption by the IT industry. The usages of live migration and security exploits over it have both increased over time.

Keywords- Cloud computing, Virtual machine, VM live migration, VM lives migration security, Attacks on live VM migration, Cryptography.

I. INTRODUCTION

Cloud computing has grown out of developments in grid computing, virtualization and web technologies. National Institute for Standard Technology (NIST) [1] defines cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud Computing offers subscription based access to Infrastructure, Platforms, and Applications that are popularly referred to as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) that helps business organizations, academic institutions, government organizations in cutting down operational expenses. The significant features of Cloud Computing include lower cost, incremental scalability, reliability and fault tolerance, service-oriented, utility-based, virtualization. Virtualization technologies can greatly, surprisingly changes enterprise client computing. Virtualization can increase agility because IT can introduce new capabilities and upgrade platforms more quickly. Virtualization can also reduce CapEx (Capital Expenditure) and OpEx (Operational Expenditure). By abstracting the OS from the hardware platform, IT can simplify service provisioning, with a reduced building time and integration cost. Virtualization also opens the door to new usage models, such as delivering the IT environment as a managed VM while letting employees use a personal device, to keep the same working environment although employee is not using a device provided and managed by IT [2].

Live VM Migration, like any other network-bound process, is susceptible to network attacks such as ARP spoofing, DNS poisoning, and route hijacking. If an attacker somehow manages to place himself between the source and the destination host, he can then conduct passive (sniffing) or active (man-in-the-middle) attacks. The fact that the live migration procedure is usually carried out inside a LAN makes it even more likely for a network attack to be successful, especially in situations where different third-parties run their VMs inside the same network subnet, which is the case in cloud computing [3].

Live migration is a useful feature and natural extension to virtualization technology that allows for the transfer of a virtual machine from one physical machine to another with little or no downtime for the services hosted by the virtual machines. It is required in many cases like online system maintenance, fault tolerance, workload balancing, testing and consolidation of VMs etc. For instance, due to resource conflict the VMs running on the same physical machine may fail to serve continuously. To avoid failover of the VMs, it becomes necessary to live migrate one or more VM running on one physical server to another physical server for continued and uninterrupted service. Live migration at present is performed manually. However, research is going on for automated live migration. Most of the commercial and open source hypervisors now support live migration. For example, VMware, Xen, KVM (kernel based virtual machine), Virtual box etc.

Most of the previous work has focused on the implementation of live migration with little or no consideration towards its security. Unfortunately, several vulnerabilities are disclosed in the implementation of live migration in Xen, VMware and etc. The major one is the

migration protocol does not encrypt migration data. All migration data, i.e. kernel memory, application state, sensitive data such as passwords and keys etc. are transmitted as clear text. Thus, there is no confidentiality of transmitting data. Other vulnerabilities migrating a VM to untrusted platforms, authentication and authorization of operations that control VM, integrity of VM data, bugs in hypervisor/migration module code etc.

A secure live migration requires

- The source and destination platforms are trusted.
- Authenticated and authorized management capabilities (VM creation, deletion, migration etc.).
- The migration data should remain confidential and unmodified during the transmission.
- Mechanism to detect and report suspicious activities.

In following sections first we will discuss issues of live VM migration and then different categories of attacks on live migration of virtual machine subsequently then after we will discuss some approaches and method to secure live migration. And in the last section we will conclude all the approaches and summarize them.

II. SECURITY ISSUES IN LIVE VM MIGRATION

Cloud computing is the internet and network based technology. There are some security threat the normally occur during the internet based transmission. As cloud computing is also depends on third network so that during the live migration of virtual machine some these threat/issues may arise which we have discussed below.

Access Control: An inappropriate and incomplete access policy over Virtual machine can lead to unauthorized user to initiate start migration, abort migration and stop the migration. An unauthorized user might insert a malicious code in the VM and can use same for getting access over other VM also can use the same VM to launch attacks and compromise destination host where it is about to migrated and getting executed.

Authentication: There is an SLA (service level agreement) between Cloud service providers and the user. User has to sign the SLA before using any service from the service provider. Cloud service providers provide services using VM. Initially VM gets distributed to multiple servers by the cloud service provider to provide services to different regions. There are multiple cloud service providers where cloud user subscribes services from multiple service providers. As a cloud service provider uses to replicate data over multiple servers, user needs to get access for each server using login credentials given by service provider. When user tries to get access he needs to provide login credential over servers and have to authenticate from each server for each service. These redundant actions may exploit user credentials over the internet.

Data Confidentiality: VM migration involves control messages need to be exchanged in between hypervisors executing on host and destination; these messages are normally in text format. As there is network involve in communication between hypervisor an intruder can easily get access over control messages and can initiate or stop VM migration. VM consists of data, when VM migration initiated the data along with the VM state need to preserve, but the pages never encrypted or decrypted the data which involves in migration appears clear text data over internet. So data gets visible to attacker where he can misuse or change content of data also can retransmit modified state data to the destination host.

Accountability: Cloud Computing needs a mechanism where the user and VM should be monitored frequently, because in case of downtime or in case where VM gets malfunctioning, the user might lose its content and can blame over service provider regarding data loss or data theft. A monitoring mechanism should be incubated over Cloud Computing where whenever VM migration process done using auto or manually log of each action from user and VM should be maintained.

Data Integrity: Data integrity is one of the major issues in VM migration. Transmitting data over the network involves intruders who can directly access data over the network. The data over network goes in the form of text, which can be easily captured over network and content of such might altered by the intruder. A packet in the network gets captured by the user and can generate a false request over network to initiate VM transmission and can halt execution of a VM.

Availability: Once an attacker gains access over physical host by finding vulnerabilities, it might initiate a large number of VM migrations to intended host where the attacker has an interest. Doing this causes the destination host to be overloaded. Overloading a host lead to downgrading performance of host and generates a large amount of traffic over network causing server down and ultimately not allowing legit imitate user to gain access over service.

Privacy: one of the features of CC is that it maintains transparency to VM migration. The VM gets migrated without user understanding users who stores data or access data from VM. The VM migration might involves passing nation boundaries; each nation has their own laws that lead to open access to user data [4].

III. RELATED WORK

3.1 Attacks In Live Migration

Attacks here are categorized on the basis of the causes that let the attack happen. The categories of attacks are inappropriate access control policies, unprotected transmission channel and loop holes in the migration module.

Inappropriate access control policies: An inappropriate access control policy allows an unauthorized user to initiate, migrate and terminate a virtual machine. The access control policy also decides access to the hypervisor, isolation between VMs on same machine and resource sharing, etc. A security lax can help an attacker to perform following attacks. DOS Attack, Internal Attack, Guest VM Attack, Inter VM Attack. To prevent an attacker from performing such an unauthorized activities appropriate access control policy (ACLs) must be defined. Access control policies define who can migrate out a VM, who can request to migrate in a VM, Who can suspend a VM, whether a user can terminate VM, and other such decisions. These ACL‘s must be authenticated and resistant to tampering. The ACL‘s can be accompanied with a firewall to check that migration is from allowed source and to allow destination systems [5].

Loopholes in migration module: Vulnerabilities in migration module are stacking overflow, heap overflow and integer overflow etc. Such vulnerabilities can be exploited by an attacker to inject malicious code or even halt the process. The system must be updated with the recent releases and patches to be protected from such vulnerabilities [5].

Unprotected transmission channel: The insecure and unprotected transmission channel is result of the migration protocol. The migration protocol does not encrypt the data as it travels over the network, thus susceptible to active and passive attacks. An attacker can gain access to the transmission channel using techniques such as ARP/DHCP poisoning, DNS poisoning and IP/route hijacking to perform passive or active attacks. Passive attacks include eavesdropping of messages for sensitive data, passwords and keys, capturing authenticated packets and replying them later. Active attacks are more serious. One solution is to assign a VM or group of VM to a VLAN. The VLAN isolates migration traffic from other network traffic and defines secure transmission channel for migration data. Other solutions include encryption of migration data to provide confidentiality integrity can be preserved using MAC, digital signatures and checksums.

IV. APPROACHES AND METHODS

4.1 Network Security Engine-Hypervisor (NSE-H)

This approach is based on hypervisors included with network security engines to eradicate intrusions occurring in virtual network [5]. NSE includes firewall, intrusion detection systems and intrusion prevention system to provide security to virtualized environment. They include intelligent packet processing capability built in them. The NSE firewall work in state full way. They maintain security context for each packet and make decisions based on security context and packet content. There are two modules in it CTM (connection tracking module) and PMM (policy matching module). The CTM keeps track of transport layer connection status using a hash-table like database. When a packet arrives it looks up the database based on packet header. If a match is found with the existing connection then accept action is executed otherwise the packet is forwarded to PMM for further decision. The PMM stores a set of packet filtering policies defined by administrator. The filtering policies are composed of

Rule sets; each rule set consists of sequence of descriptors that are matched with packet content and the action to be taken.

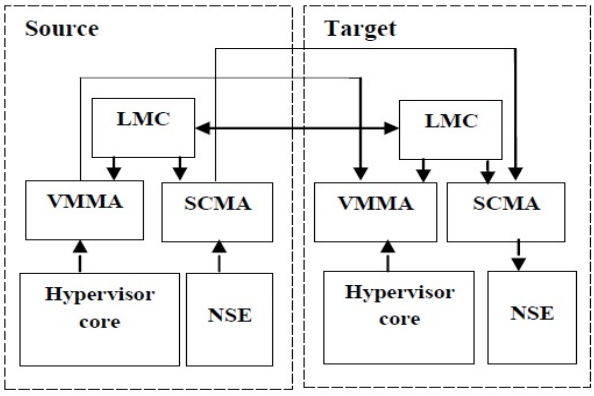

Figure 4.1 NSE Framework Architecture

Virtual machine migration agent (VMMA) interacts with the destination hypervisors‘VMMA to transmit the VM encapsulated states to the destination hypervisor.

Security context migration agent (SCMA) encapsulates and sends VM related security context set through a dedicated channel.

Live migration coordinator (LMC) collaborates with destination hypervisors‘LMC and schedules the two agents to perform migration tasks in parallel.

4.2 Role-based live migration

After building the trustworthy virtual machine container, one session for the virtual machine migration will be started as shown in Figure 4.2. A VM will be either migrated to a host, or migrate out from the host.

Migrate-out: (flowchart with green lines): The owner of a VM initiates one outgoing request to the migration service module. This service checks whether this move is allowed by checking the policy service module, which makes migration permission according to pre-deployed policies for this virtual machine. After the migration service gets the "Allow" permission from the policy service module, it gets key and certificate from the seal storage module to encrypt the entire state of the virtual machine, and then migrates the virtual machine to the targeted platform [2].

Migrate-in (flowchart with red lines): The owner of VM initiates one incoming migration request to the migration service module. At the mean time, policies regarding to this VM are loaded. After validating the policies, the policy service module stores it to his local environment in seal storage [2].

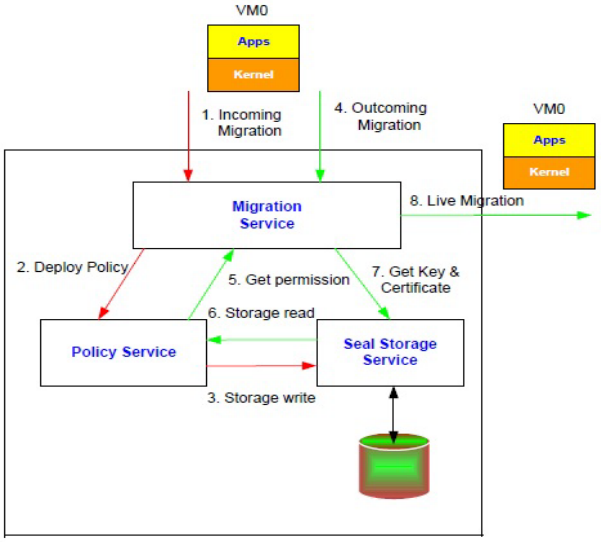

Figure 4.2 Role Based Access

4.3 Secure Hypervisor:

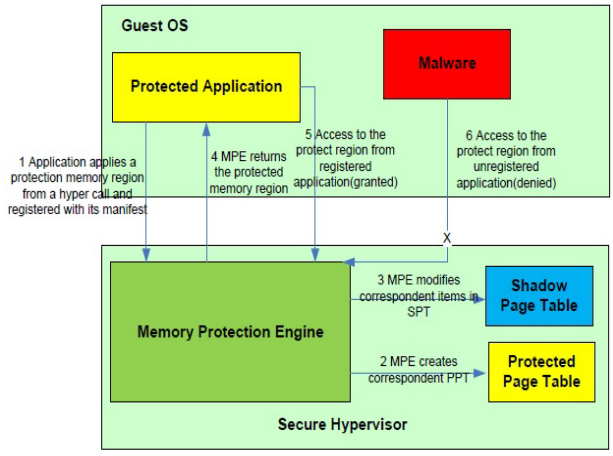

Figure 4.3 Secure Hypervisor

Finally, the overall secure framework uses a secured hypervisor design that provides the protection on key applications in a Guest VM. We adopt the work in and to provide runtime memory protection. In this proposal, we utilize hardware techniques to provide trust services to software programs. Without modifying OS, we leverage Intel vPro technology to create a lightweight hypervisor for fine-grain software runtime memory protection. As a result, a program's memory could be hidden from other high-privilege system software's in a single commodity OS [2].

V. CONCLUSION

Table 5.1: Comparison of discussed approaches.

Parameters	NSE-Hypervisor Approach	Role Based Approach
Confidentiality and Integrity of VM during migration	NO	NO
Authenticated and authorization of migration operation (Access Control policies)	Yes	Yes

To conclude no any approach discussed above is available that addresses Confidentiality and Integrity of migration data, Authentication and authorization of migration operations which is the need of secure migration. Therefore there is a need to derive a method which provides and satisfy all the security parameters.

6. REFERENCES

[1] Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, September 2011.

[2] Wei Wang, Xiaoxin Wn, Ben Lin, Kai Miao, Xiaoyan Dang, "Secured VM Live Migration in Personal Cloud" Intel Labs, Intel Information Technology, at intel.com.

[3] Diego Perez-Botero, "A Brief tutorial on Live virtual machine migration from a Security perspective", Princeton University, Princeton, NJ, USA

[4] Ssuresh B. Rathod, V.K. Reddy, "Secure Live VM Migration in cloud Computing: A Survey", International Journal of computer Applications(IJCA) Vol.103-No.2 October 2014.

[5] Jyoti S, Anala M R, Shobha G, "A Survey on Techniques of Secure Live Migration of Virtual Machine", International Journal of computer Applications(IJCA) Vol.39-No.12 February 2012.