

Security Issues in Live Migration and Survey of Existing Solutions

Jahanvi Kolte¹ Rujul Solanki² Shams Narsinh³ Hardik Solanki⁴

^{1,2,3,4}Institute of Technology, Nirma University, Chharodi, Ahmedabad, Gujarat, India.

Abstract— Live migration was introduced to support many features of cloud computing like workload balancing, fault tolerance, online system maintenance, consolidation of virtual machine, etc. Live Migration is transferring of VM from source host machine to destination host machine while being powered on. Cloud has various key points which can be exploited by attackers. As cloud is prone to security attacks, it is necessary to ensure secure transfer of VM. This paper discusses the process of live migration, various security attacks possible along with their effects and some solution to maintain security in live migration.

Keywords: Virtualization, Live Migration, Virtual Machine Monitor, Hypervisor, Man in the middle, Denial of Service attack.

I. INTRODUCTION

Virtualization has opened new doors for efficiently utilizing computing power and storage. The concept of virtualization was basically introduced for maximizing utilization of the expensive hardware resources of mainframe systems which were underutilized at that time. To achieve this, techniques such as multiprogramming and timesharing were developed. These techniques formed the basis of concept of —virtualization.^[1] The scope of virtualization has expanded over time and now it is used in wide areas such as Cloud Computing, Grid Computing, Utility Computing, etc. Recent advances in virtualization have made virtual machines an increasingly important research and operational area.^[2]

Virtualization is abstraction of hardware resources, operating systems, storage devices or computer network resources. Virtualization can be used to share a computer system among multiple users, to isolate users from each other and control program, to emulate hardware on different machine, etc. Live migration is essential feature of virtualization defined as a process of dynamically transferring running VMs from one physical server to another with little or zero downtime and without interrupting services running in VM[3]. Live Migration facilitates proactive maintenance in case of failure. It can also be used for load balancing to optimize the utilization of available resources. In failure prone systems, it is necessary to live migrate data to another physical server so that data loss can be prevented and service can be obtained continuously.

There are several vulnerabilities in live migration like lack of migration protocol that encrypts migration data, migrating VMs to untrusted vendors, authentication and authorization of operations, integrity of VM data, Denial Of Service(DoS) attack, etc.

II. BACKGROUND

Live Migration allows CSP to transfer running instance of VM from one machine to another machine. It enables dynamic scalability, load balancing, backup with a little downtime of milliseconds.

A. Process of Live Migration

The live migration process comprises of several steps explained as follows.

1) Pre-Migration

These are the tasks that must be ensured prior to migration. In this step, a VM is running on host machine. Alternate VM is selected for migration and it is ensured that it has the required resources are available. The VM container on the alternate host should be able to fulfil the requirements of the customer.

2) Reservation

In this step, a request is sent to the alternate server to migrate a VM from one host machine to another host machine.

3) Iterative Pre-copy

In this step, all pages are transferred from source host machine to destination host machine. In the rest of the iteration all the pages which are modified or dirtied during previous iteration are transferred.

4) Stop and Copy

In this step, the source host machine is suspended and all the dirtied pages are transferred to the destination host machine which results into consistent copy of VM at both host machines. The copy at source is considered primary in case of any failure.

5) Commitment

The destination host machine acknowledges the received consistent OS image by sending message to source host machine. The source host machine interpreting that message as commitment of migration transaction discards the original VM and destination host machine becomes the primary host.

III. ATTACKS ON LIVE MIGRATION

Live Migration is subjected to many weakness which can be exploited. Several kinds of attack are possible on live migration. Some of them are as listed below.

A. Denial of Service attack

In this attack the outgoing migrations can be initiated by an unauthorized attacker who can direct them onto target host server which results in overloading of the server. Due to overloading, the server performance decreases and service can also be disrupted. Attacker can go other way and migrate from server to server resulting in reduction of performance of service provided by VM.

B. Man in the middle

This type of attack takes its name from a malicious intruder trying to intercept the message with an intent of listening it or modifying it. In man in the middle attack the attacker spoofs the IP address of the host and destination machine and redirects all the data through his/her machine. There are two types of man in the middle attack.

1) Active attack:

In active man in the middle attack, attacker tampers the incoming data from source host and sends tampered data to destination machine.

2) Passive attack:

In passive man in the middle attack the attacker just listens or sniffs the data collecting critical information like password, confidential data, etc.

C. False Resource Advertisement

An attacker can falsely advertise resources influencing VM migration to his host machine. When a request for new VM is generated during live migration, an intruder may intercept the message. Although destination VM may not have enough resources, the intruder can advertise that destination has available resources. The destination VM host is requested only the possible allocation of resources so destination also accepts the request. Now during live migration, as enough resources are not available or capacity is over flown, the system may plunge into some inconsistent state. Moreover, if the intruder owns the destination host, he/she can receive entire data of user.

D. Blocking message for releasing resources

Once the stop and copy phase is completed, the new VM host now initiates a message asking the old VM host to release its resources. If an intruder blocks this message and confirms status to destination host on behalf of source host, destination host thinks live migration is completed and now it may proceed further with its operations. On the other side, due to lack of acknowledgement source host thinks that live migration failed. So, the previous instance of VM is also allocated and the user is unaware about it. All critical data like authorization details can be obtained during live migration. Now the intruder can use the previous instance of VM allocated to the user after entering authorization details. The actual owner of VM will be charged for utilization of resources by the intruder. If the model follows a post utilization payment method, the actual owner might know this quite later.

E. Blocking acknowledgement of data

Once data is being transferred either in iterative per copy or stop and wait phase, it needs to be acknowledged by the new host. If the intruder blocks this acknowledgement, the source host thinks that there was some transmission error and retransmit the same message again and again. The destination host acknowledges it but the acknowledgement does not make its way back to source host. This reduces the system performance. If no mechanism is maintained to detect duplicate packets, the destination host will be inconsistent as per the user requirement.

F. VM zombie

The attacker can attack and gain control over source host and initiate migration to other host without the knowledge of user. The source host in this case acts as a VM zombie.

G. Gaining control over target Hypervisor

An attacker might gain unauthorized control over the hypervisor and may lead to malicious VM management. For example, not allowing a particular VM to be scheduled, not

updating the VM copy, retrieve confidential details, initiate migration, etc.

H. Inter VM Attack

The VMs running on same machine can communicate with each other. If some policy is not defined for controlled communication, a malicious VM can attack other VM running on same machine.

I. Internal Attacks

This can be result of unauthorized attacker migrating VM with malicious code to legitimate target hypervisor. This provides a platform for malicious VM to perform internal attacks on target system. For example gaining control over the target hypervisor and other guest VMs.

IV. POSSIBLE SOLUTIONS

Some of the solutions that ensure secure live migration are explained below.

A. Isolating the migration traffic

To isolate migration traffic, assign a small group of VMs to its own host based VLAN. The VLAN defines a secure transmission channel for migration.

The problem with the above approach is the complexity and cost involved as the number of VM grows.

One approach to secure live migration against all attacks discussed is to assign a small group of VMs or even a single VM to its own host-based Virtual LAN (VLAN). VLAN is basically a segmentation and isolation tool. The VLAN isolates migration traffic from other network traffic and defines a secure transmission channel for migration. The complexity lies in setting up and maintaining VLANs for each VM, synchronizing VLANs configuration on virtual and physical switches, troubleshooting and fix configuration errors, manage the growth and complexity of acls as number of VM increases, ensure compatibility between physical network and virtual network security policies.

Host-based VLANs can't provide security when more than one VM is assigned to a given VLAN. There is no traffic monitoring and filtering mechanism thus inter-VM communication within the VLAN remains invisible.

B. Network security Engine-Hypervisor (NSE-H)

The hypervisors includes a network security engine to prevent intrusion from taking place in virtual network. NSE includes firewall, intrusion detection system, and intrusion prevention system that helps to secure the virtual environment.^[1] NSE makes decision based on security context and packet content that it keeps track of NSE consists of two modules: CTM(connection tracking module) and PMM(policy matching module).

Whenever a packet arrives it first passes through CTM phase which keeps track of transport layer connection with help of hash table like database. If the packet header matches with existing connection then it is executed otherwise it is forwarded to PMM phase.

In PMM phase the packet is passed through packet filtering policies defined by administrator based on content of the packet. If the packet content passes through all these

filters successfully then it is accepted otherwise it is dropped.^[1]

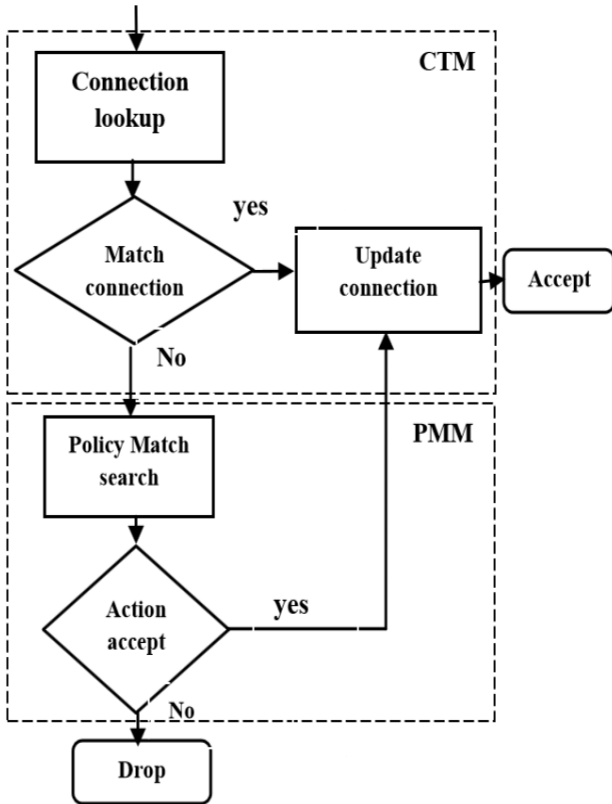


Fig. 1: Stateful firewall workflow

Whenever a packet arrives it first passes through CTM phase which keeps track of transport layer connection with help of hash table like database. If the packet header matches with existing connection then it is executed otherwise it is forwarded to PMM phase.

In PMM phase the packet is passed through packet filtering policies defined by administrator based on content of the packet. If the packet content passes through all these filters successfully then it is accepted otherwise it is dropped.^[1]

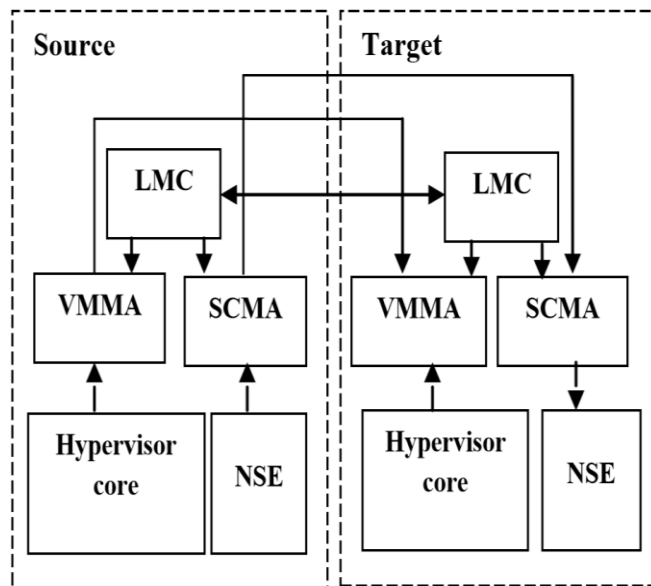


Fig. 2: CoM Framework Architecture

The process of live migration encapsulates only the execution context and not the security context for transmission due to which the VM gets rejected for not matching required security context. To overcome the security context problem CoM framework is proposed

Virtual Machine Migration Agent (VMMA) transfers VM encapsulated states to destination hypervisor by interacting with destination hypervisor's VMMA.

Security Context Migration Agent (SCMA) solves the problem by encapsulating the security context and sending it through a dedicated channel.

Live Migration Coordinator(LMC) schedules two agents to perform migration tasks in parallel by collaborating with destination hypervisor's LMC.

Live migration in CoM:

Preparation: VMMA and SCMA reserves the resources and gets ready for migration as the LMC on the source informs LMC on destination to do so.

Iterative synchronization: The SCMA transfers security context of VM while VMMA transfers execution context iteratively to the destination.

Final synchronization: The modified pages are migrated after first phase of synchronization. The migrated VM is then suspended on the source hypervisor and the traffic related to VM is redirected to target server.

Resumption: The source discards VM instance and migrated VM is resumed on target hypervisor.

C. Role Based Migration

The following modules are included in role based migration which is based on use of Intel vPro and TPM hardware.

Attestation service: In this module process of cryptographically identifying hypervisor is done by other hypervisor to establish trust.

Seal Storage: Storage of private key and role based policies are done in this module. It encrypts the data which is responsible for attestation using private key of TPM. Encrypted data also includes hash of the booted OS so that TPM allows OS with same hash to unseal it.

Policy Service: The management and parsing of role based policies are done here.

Migration Service: This module makes sure that target machine meets security requirement before migration after it initiates attestation requests to remote host.

Secure Hypervisor: Process of guest OS is protected by this module by Runtime memory measurement. The design uses remote attestation to see if the target VM meets the require specification.

Migration session starts after successful attestation. Each migration request whether its outgoing or incoming must satisfy role based policy defined by admin.

Hence the role based migration defines mechanism for platform attestation and a mechanism for defining role based policies for live migration

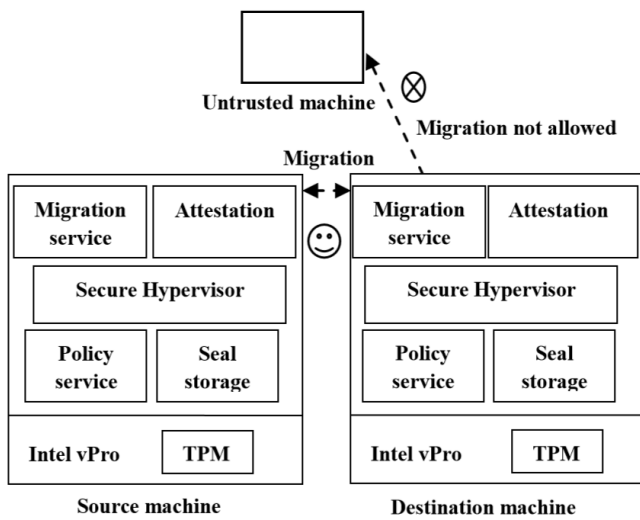


Fig. 3: Architecture of Secure Live Migration.

V. ANALYSIS

The NSE-H based approach enables transfer of security context along with migration data that enables it to provide features of security like firewall, IDS, IPS inside NSEs. The policy based approach establishes trust through attestation process, defines role based migration policies ensuring that authorized user can perform migration operations.

VI. CONCLUSION

Live Migration is an efficient technique that enables proactive maintenance of VM. It can be used for load balancing on the server. Live Migration must be used regularly on failure prone systems so that no data is lost. As live migration is prone to security attacks, secure transmission of data is very important. As far as secure approaches are concerned, there is no approach available to securely perform live migration. None of the above discussed approaches address Trust establishment, Confidentiality and Integrity of migration data, Authentication and authorization of migration operations which is the need of secure migration.

ACKNOWLEDGEMENT

We wish to thank Prof. Madhuri Bhavsar for giving us the opportunity to work on this dynamic topic of Security Issues in Live Migration which witnesses wide applications in many crucial areas of decision making. I would also like to convey my deep appreciation for her support and guidance throughout the project.

REFERENCES

[1] Jyoti Shetty, Anala M. R., Shobha G., *A survey on Techniques of Secure Live Migration of Virtual Mahine,* International Journal of Computer Applications(0975-8887), Volume 39- No. 12, Feb 2012

[2] Jon Oberheide, Evan Cooke, Farnam Jahanian, *Empirical Exploitation of Live Virtual Machine Migration,* Proc of Black Hat DC, March 24, 2008

[3] Chen Xianqin, Gao Xiaopeng, Wan Han, Wang Sumei, Long Xiang. *Application- Transparent Live Migration for virtual machine on network security enhanced hypervisor,* China Communications.

[4] Alternatives for Securing Virtual Networks: A Different Network Requires a Different Approach— Extending Security to the Virtual World. white paper 1000220-012-EN Dec 2011, Juniper Networks, Inc.

[5] Gerald J Popek and Robert P Goldberg. *Formal requirements for virtualizable third generation architectures.* In SOSP '73: proceedings of the fourth ACM symposium on operating system principles page 121, 1973.

[6] Melvin Ver. *Dynamic Load Balancing Based On Live Migration Of Virtual Machines: Security Threats and Effects.* Thesis report Rochester Institute of Technology, B. Thomas Golisano College of Computing and Information Sciences (GCCIS), Rochester, NY, U.S.A.

[7] Christopher Clark, Keir Fraser, Steven Hand, Jacob Gorm Hanseny, Eric July, Christian Limpach, Ian Pratt, Andrew Warfield, *“Live Migration of Virtual Machines”*, in NSDI 2005.