
Rajesaheb R. Kadam¹, Manoj Bangare²
Department of Information Technology, SKNCOE Pune, University of Pune, India.
rajekadam2010@gmail.com, manoj.bangare@gmail.com

ABSTRACT

Virtualization technology allows the sharing of same physical resources among several users and helps to achieve optimum utilization of physical resources. Hardware virtualization is the process of partitioning the physical machines into logical machine using virtualization software called hypervisor and each logical machine is called virtual machine (VM). Live Virtual machine migration is the process of transferring a virtual machine from one physical machine to another while the VM is running and without interrupting the services running in VM. Live migration helps System administration in fault tolerance, online system maintenance, workload balancing and consolidation of VMs etc. However, vulnerabilities associated with live migration pose many security threats. Because of these threats IT industry is hesitate to adopt live migration for sensitive data applications. This paper is a survey of attacks on live migration of virtual machine and approaches to handle them. This paper also discusses proposed strategy to secure live migration.

Index Terms : Virtualization, Virtual Machine, Live Migration, Security, Hypervisor.

I. INTRODUCTION

Virtualization technology was introduced in late 1960s by IBM. At that time the expensive and powerful mainframe computers were used for computation purpose but these mainframe computers were underutilized. Hence to optimize the utilization of most expensive hardware components and resources, multiprogramming and timesharing techniques were developed. Multiprogramming and timesharing formed the basis of virtualization. Virtualization is the technique which divides physical machine into several completely isolated machines known as virtual machines. Virtualization is the abstraction and emulation of hardware resources to have better resource sharing. We can have different types of virtualization such as server virtualization, operating System virtualization, Hardware emulation, paravirtualization, storage virtualization, network virtualization, Full virtualization etc [2]. Thus virtualization reduces investment, installation and operational cost for enterprises.

The server virtualization or system virtualization is the ability to run multiple virtual machines, including their operating systems called Guest Operating System on existing real operating system called Host operating System. Virtual machine is an efficient isolated duplicate of real machine [3]. Virtual machine monitor (VMM) is a software abstraction layer that isolates the virtual machines by emulation of hardware. VMM is also called as hypervisor which controls the creation of VM and have control over all VM and system resources.

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 [4]. Downtime is the total time for which VM stops running. Live migration helps System administration in cases like fault tolerance, online system maintenance, workload balancing and...
consolidation of VMs. Also in case of natural disasters Live Migration plays very important role in recovery process. Limited resources on same physical machine running multiple VMs causes resource conflict due to which physical machine may fail to serve continuously. Hence, to avoid failure of VMs live migration is the solution to have continued and uninterrupted service. At present live migration is performed manually. Most of open source hypervisors like VMware's (VMotion), Xen, KVM, Oracle's Virtual box etc supports live migration. Up till now most of work is focused on live migration of VM with little consideration towards security. There are several vulnerabilities are present in the implementation of migration in Xen [5]. Migration protocol used is not secure and does not encrypt migration data of VM. Hence, there is no confidentiality of migrated data and other vulnerabilities like untrusted platform, authentication and authorization, bugs in hypervisor code etc.

A secure live migration of VM requires Trusted source and destination platforms, authentication and authorization mechanism, confidentiality and integrity of migrated data, Mechanism to detect and notify suspicious activities.

II. ATTACKS

Detection of live virtual machine migration process plays important role while conducting attacks on it. Virtual machine live migration detection has been demonstrated in [6] using ICMP packets. [7] Provides a comprehensive survey of vulnerabilities leading to attacks in Live Migration. They are categorized into inappropriate access control policies, unprotected transmission channel, loopholes in migration module etc.

A. Inappropriate Access Control Policies

Inappropriate access control policies allow any user to initiate migration and terminate migration of virtual machine. Access policies also control access to hypervisor, isolation of VMs and resource sharing. Because of this attacker can exploits attacks like denial of service attack, Man-in-middle attack, Guest VM attack, internal virtual machine attack. Using loopholes in access policies attacker can migrate malicious VM to hypervisor and malicious VM harms the hypervisor and other VM instances [7].

B. Unprotected Transmission Channel

Unprotected transmission channel is the result of insecure migration protocol. Insecure migration protocol does not encrypt the data flow over network and vulnerable to active as well as 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 [6]. Passive attacks are eavesdropping of messages for passwords, sensitive data and capturing authenticated packets. Active attacks are manipulating kernel memory, manipulating authentication services like /bin/login, sshd etc.

C. Loopholes in Migration Module:

Loopholes in migration module are stack overflow, heap overflow and integer overflow which makes the migration vulnerable. Oberheide et al. developed a tool named Xensploit [8] to carry out man-in-the-middle attacks on virtual machine migration. Xensploit was used to modify the memory segment, specifically the sshd memory segment, in such a way that the sshd authentication was be bypassed. Virtualization software is having large number of LOC and complex. Xen hypervisor has about 200K LOC and XEN emulator has about 600K LOC and the Host has about 1K LOC [9]. With this large LOC bugs tends
to exit. Bug reports such as those listed in NIST’s National Vulnerability Database [10] show the difficulty of shipping bug-free hypervisor code. By exploiting these attacks, attackers can have access to virtual machines and breach the confidentiality, integrity of virtual machines’ data.

III. Solutions for Secure Live Migration

Following are the solutions for preventing attacks in live migration:

A. Virtual Local Area Network

VLAN is one of the Approaches to have secure live migration by isolating migration traffic and assigning group of VMs to VLAN. VLAN is virtual network created inside a public network and it is independent of physical location created by assigning tag to the packets with tag-ID of corresponding VLAN [7]. VLAN defines a secure and trusted transmission channel by isolating migration traffic from other network traffic. A major drawback of VLAN-based security approach is the growth in complexity and administrative costs as the VM population grows [11]. The complexity lies in maintaining and setting up VLANs for each VM, troubleshooting and fix configuration errors, synchronizing VLANs configuration on virtual and physical switches, ensure compatibility between physical network and virtual network security policies, manage the growth and complexity of acls as number of VM increases.

B. The CoM Security Framework and Network Security Engine:

Network Security Engine is a security module based on the hypervisor including protection mechanisms like firewall, IDS and IPS. The CoM framework is based on both hypervisors and network security engine (NSE), thus system is called Network Security Engine-Hypervisors [4]. NSE includes intrusion detection system (IDS), intrusion Prevention System (IPS) and firewall which provides security to virtual environment. The NSE firewall has built in packet processing capability and works in a state-full way. The CoM framework provides traditional security approaches like IDS, firewall, IPS to have secure live migration. In this approach security context and migration data is encapsulated and transferred so that VM is restored on destination.

C. Role Based Migration:

Role based migration process based on Trusted Platform Module hardware and Intel vPro. In this TPM hardware is used to find cryptographically trusted remote hypervisor for secure migration. Trusted platform module (TPM) functionality can be powered in several other ways as well for secure virtual machine migration. TPM can recognize the presence of unauthorized and illegal access to the system. [12] Created a software module named vTPM inside the hypervisor, to share the TPM functionalities with the OS running in each virtual machine. For each virtual machine, an instance of TPM module (vTPM) is created. However, [13] points out that as this implementation is completely inside the software, it cannot protect the cryptographic secrets in every operating system.

D. Comparison of Solutions
In live migration process there are several authentication issues as well as active and passive attacks which exploits live migration process. The main cause of this is lack of secure live migration protocol. Hence secure live migration protocol should be used for live migration having essential features like protected transmission channel, integrity of migration data and entity authentication [1].

IV. RELATED WORK

In Process migration, process moves from one physical server to another physical server. In 1980’s more research was done in process migration. However, due to residual dependency process migration didn’t get popularity [16]. OS migration is another approach which handles all limitation of process migration and does the virtual machine migration efficiently. OS migration overcomes the residual dependency problem and administrator need not worry about it. Administrator can migrate OS and its associated process as single unit.

Main theme of VM migration is to migrate memory and control of VM from one physical server to another without any service interruption. More research has been done in memory page migration process. Memory migration [16] process can be described as:

- **Push phase:** Certain memory pages are pushed to new machine while source VM continues running without stoppage. To ensure consistency between memory pages, pages which are modified are re-sent.

- **Stop-and-Copy phase:** The source VM is stopped, transferred to destination and only started at destination host after all memory pages are copied at destination host.

- **Pull Phase:** If destination machine access memory page which is not yet copied to destination from source machine, those pages are faulted (“pulled”) in across the network from source VM.

Stop-and-Copy is one of the best approaches of memory migration which involves stopping the original VM, copying all memory pages to the destination, and then starting the new VM. This approach has advantage of simplicity but both downtime and migration time is proportional to the amount of memory allocated to VM. Hence, to have minimum downtime pure demand migration was adopted which uses Stop-and-copy phase. In this approach the kernel data structures are copied to destination machine and the new VM started at destination after complete migration of memory pages. The remaining pages are fetched to destination at first use. This leads to less downtime but increased migration time also increased total migration time due to frequent page faults. Another best option of VM migration is pre-copy migration. The pre-copy approach provides a best way of migration by combining iterative push phase and a short stop-and-copy phase [16]. Memory pages are copied in rounds called iterative coping.
The memory pages which are modified in first round are copied in next round. Every VM has set of small number of pages which are frequently modified which are poor candidates of pre-copy migration. The writable working set was designed to calculate total number of iterative for particular workloads.

Wide research has been done to make live migration secure with efficient and minimum downtime. Live migration can be done from one server to another located in same room which has physical security and less chances of data loss. As increased popularity and demand of virtualization live migration was performed in LAN, from one physical host to another located at different physical location. Due to this physical separation physical security is not possible which invites data sniffing and other threats to live migration process. It is observed that live migration is vulnerable to Man-in-the-Middle attack. By exploiting this attack any unauthorized user can sniff the ongoing data and visualize the data. The traffic ongoing on data plane is sensitive and not secured. Using tool Xensploit several attacks on live migration were evaluated and associated into different modules like control plane, data plane, migration module. Hence, to have data confidentiality and integrity we need to use secure migration protocol [1].

V. PROPOSED SOLUTION

Security measures to protect sensitive data during live migration should be designed in such a way that data confidentiality and integrity is preserved. IPSec tunnel is one of the ways to secure live migration as discussed below:

A. IPSec Tunnel

IPSec protocol is the secure protocol in network layer and used for securing the internet protocol traffic. By building IPSec tunnel we can have secure live VM migration through tunnel. If live migration is done through Internet protocol security tunnel, then we need to face the problem of increased downtime of VM. This increased downtime cause service disruption but have secure live migration since data will be encrypted. While passing of data through tunnel authentication and encryption of each IP packet is done. In [17], author gives detail explanation of operations, authentication and encryption techniques. We can use IPSec tunnel to protect data flow at server-to-server levels or from edge router-to edge router. Hence, if live migration is done through IPSec tunnel, IP packet would be encrypted and difficult to sniff data and trace it.

![Figure 1. Live VM migration through IPSec tunnel](image)
VI. CONCLUSION

In this paper, we have discussed various vulnerabilities and associated attacks on live migration and also discussed various approaches to tackle with these. It is concluded from the survey that the main cause of these vulnerabilities is insecure migration protocol and no single integrated approach is available which provides platform integrity verification, Confidentiality and Integrity of migration data, Authentication and authorization of migration operations. Hence, we have proposed strategies which suggest that secure live migration should be done through IPSec tunnel with strong encryption techniques.

VII. REFERENCES


AUTHOR PROFILE

Rajesaheb R. Kadam: Student, M.E Department of Information Technology, Smt. Kashibai Navale College of Engineering Pune, Savitribai Phule Pune University, India

Manoj Bangare: Assistant Professor, Department of Information Technology, Smt. Kashibai Navale College of Engineering Pune, Savitribai Phule Pune University, India.