Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 55 – 60

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

A Study on Security Vulnerability on Cloud Platforms

Santosh Kumar Majhi[a,b,*], Sunil Kumar Dhal[b]

[a]*Veer Surendra Sai University of Technology, Burla, India*
[b]*Sri Sri University, Cuttack, Odisha, India*

Abstract

Cloud computing provides an in-built platform to the users with easy and on-demand access to different system level services for creating virtual machines (VM) with efficient utilization of hardware, computing and network resources. This allows users to remotely execute large number of applications across various domains such as, health-care, utility services, e-governance, etc. There are different cloud operating platforms for creation and management of virtual machines through various system or application services. For example, openstack, oracle virtualbox, Microsoft HyperV are widely used operating platform. Virtual machine migration (VMM) is one of such important system services that used for smooth the progress of system maintenance, load management, fault tolerance, secure and safe service offerings. Virtual Machine live migration service transfers an active VM from one physical machine to another across different data centres. It involves a sequence of operations in iteration for migrating execution context of a VM to the destination machine. These operations are dependent on schedule, availability of resources and overall timing constraints. On the other hand, the migration process involves transferring the control data over a communication channel with a shared storage. Due to the above mentioned complexities of VM migration process, any security failures during the migration may cause transfer of incorrect VM instance to a data centre and which in turn may lead to exposure of the data centre to the attackers. This may be manifested as catastrophic system failure, degradation of system performance, load balancing and in long run may result collapse of the data centre. In this paper we studied various security vulnerability in different cloud platforms. These vulnerability will help the security developers to design a secured cloud platform.

*Keywords:*Cloud Computing; Virtual Machine; Cloud Operating Platform; Security Failures; Security Vulnerabilitys

* Corresponding author. Tel.: +91-9438403651
E-mail address: santoshism9@gmail.com

doi:10.1016/j.procs.2016.02.010

1. Introduction

The open and multi-tenant computing platform with remote execution of application, sharing of resources, dependency with underlying networks with fine-grained accessibility opens up various functional and security threats in cloud platform.

Security Challenges in Cloud Computing Platform: Virualization is the key enabler of Cloud computing platform to emulate the system behavior in virtual machines. In addition, the key agents of the cloud platform includes hypervisor, Virtual Machines (VMs), Operating systems in VMs, software running on those OSs and the underlying communication network. Security, in the context of computing platform, refers to the exposé and modification of data and services which may be considered responsive. Sensitive or responsive data are (i) software data (program data in memory, on disk, or in other forms of storage); (ii) software and hardware operational state (resource allocation levels, program execution paths, etc.); (iii) control and network channels. Here software refers to the hypervisor, VM, OSs in VMs and applications running in VMs[6].

Security in Cloud Network Infrastructure: VMs are protected using various security mechanisms including firewalls, intrusion detection and prevention, IPsec VPN, etc. While VMs migrate around, not only the memory and the states on the hypervisor need to be migrated, but also the network states including security policy. Failing to do so, may expose the running services on the migrated VM to security problems. A simple example of this case is firewall access control lists (ACLs). Assume that a VM migrates to a new location under a different firewall configuration. On one hand, if the ACLs at the new location are more permissive than those at the original location, some packets that should be blocked may be allowed. This may open up several security vulnerabilities to the VM. On the other hand, if they are less permissive, some packets that should be allowed may be blocked. Furthermore, some virtual machines running services might require specific filtering rules. As VMs are vigorously and frequently transfered between hosts, manually managing the complex firewall rules can be time-consuming and error-prone. The similar issue arise when dealing with intrusion detection and preventions configurations as well as IPsec VPN settings. Furthermore, scale and complexity of data centers are continually increasing, which makes it difficult to rely on the administrators to update and validate the security mechanisms.

Challenges in administration and planning level: The complex operations in cloud computing is handled by proper administrative planning. In some of the operations though the administrator has control, still there are vulnerability exists. For example, the VM Migration auction process involves a sequence of communications performed through an in-secured channel i.e, Internet, it is prone to various security breaches. The VM migration auction involves multi party receiver and each CSP controls the migration auction by running a distributed biding application. Thus, auction process may expose the cloud services especially migration process to integrity and confidentiality attacks. This may in turn lead to Denial-of-Service (DoS) attacks. On the other hand, incorrect authentication and agreements between CSPs and host-level security mis-configurations may allow attackers gaining control of target hosts and the underlying network infrastructure. Moreover, due to weak cryptographic mechanisms traffic can be captured and tampered during the communications between CSPs by running cryptanalysis techniques which in turn lead to data loss.

2. Literature Review

In this section, we present the literature review with respect to three main axes of research that can be connected to our work: Virtual machine migration in cloud computing, analysis of security context in VM migration, and VM migration planning with respect to security, capacity requirements. In addition, we have discussed policy consistency analysis initiatives for detecting and resolving anomalies and conflicts within a given security policy configuration. In the following, we will present some of the most relevant contributions in all three research areas. Ashino et al. presented EDAMP method for VM migration between heterogeneous hypervisor implementation[1]. To the best of our knowledge this is the only work which considers VM migration problem in heterogeneous cloud environment. Since we analyze the live migration problem in heterogeneous hypervisor implementation, here we present a brief description of the EDAMP method. The various phases of VM migration under EDAMP are as follows. In initialization phase, this method installs an uniform OS distribution on all VMs. EDAMP generates a local list to identify a set of files in each VM. This list contains information about each file on the virtual HDD that includes the file path, file size, and time stamp attached to the VM. After this phase, the method generates a shared list that includes various attributes of shared files used by different VMs (the shared list creation block).To generate this shared list, hypervisor has to integrate the lists from different virtual machines. In the next phase the source and destination VM are identified. In this phase, hypervisor also assigns the required resources to the source and accordingly the local VM list is updated. After this, EDAMP generates migration data by finding a difference set Ls - SL, where SL indicates the shared file list between source and destination VM at time t (initiation phase) and Ls is the local file list of source VM at time after resource allocation. In deployment phase, the required resources are installed based on the migration data file under the control of destination hypervisor. This allows the OS to boot up in the destination. In this approach, the authors discussed only about the VM state migration. However, there was no discussion regarding security context migration.

Saeed et al.[2] described a formal approach for the virtual machine migration planning that is to find a sequence of migration steps such that all security, dependency and performance requirements are satisfied. Migrating VMs in an arbitrary sequence may violate the above discussed requirements. The authors discussed the VMM-Planner, a framework that finds a sequence of migration steps in which the current VMs placement converges to the target placement without violating dependency, risk, and capacity requirements. VMM-Planner encodes VM migration planning problem into a constraint satisfaction problem in which all requirements, the current cloud status, and the target placement are formally encoded as constraints. Then, the modelled constraints are fed to a satisfiability modulo theory (SMT) solver. The solver finds a satisfiable solution to the given instance, if such solution exists. The provided solution is the VM migration sequence that can be performed to execute the live VM migration process safely. From our analysis, we have observed that (i) security context are not incorporated in VMM planning. (ii) the migration sequence does not tagged with time (iii) Only serial sequencing of migration steps are discussed, But, the parallelization of migration steps may be considered for improving system performance. (iv)The affect of functional faults and security violations in each step of VMM plan has not been analyzed.

Network elements such as stateful firewalls contribute in enforcing security in Cloud platform. During VM migration the security enforced to the VM, need to be transfered to the destination machine. Zahra et al[3] presented a framework for security context migration in a firewall secured VM environment. In their work, the security context transfer approach along with implementation has been discussed. The Security Context (SC) module in the hypervisor extracts SC of source VM and transfer the SC to destination host along with VM state. SC migrator establishes a connection (TCP) between source and destination. At the destination side, the SC module enforces the security context. Authors evaluated the work using three test case scenarios. In the first test case, a VM migration was performed without any SC information. In the second test case, a VM was migrated with static SC information. In the third test case, migrated a VM with static and dynamic SC information. The test cases are not enough to proof the correctness and consistency of the security context migration. In addition, this method consider IP address does not change after VM migration to a different host.

Researchers developed a way for an attacker to gain administrative control of some cloud platforms during a live migration, employing a man-in-the-middle attack to modify the code used for authentication. Jon Oberheide et al.[4] demonstrated the importance of securing the VM migration process. The authors classified the threats into control plane, data plane, and migration module threats. The authors developed a tool, Xensploit, to perform man-in-the-middle attacks on the live migration of virtual machines. The tool operates by manipulating the memory of a VM as it traverses the network during a live migration. Simple Memory Manipulation and buffer overflow attacks are demonstrated in XEN platform. The authentication process in VMware Virtual Infrastructure was exploited by sshd Authentication Manipulation.

Cloud Calculus[5] is a formal framework to express and verify the VM deployment and migration process in the cloud from the security point of view. More precisely, this framework allows expressing the deployment and migration of VMs along with their related security policies, and then verifying the preservation of the security after migration. This paper only discuss about the firewall rule verification and migration. However, the security context related to other security devices are not presented. The security policy mis-configurations verification in the cloud data centers are not discussed.

In this paper, our main focus is to define the various vulnerability in different cloud operating platforms. In the next section , we listed the vulnerability considering Xen, Virtualbox and HyperV virtualization techniques.

3. Vulnerability in Various Platforms

3.1. Xen

Control plane attack: The entire state of the virtual machine is exposed to the device module or the hypervisor and if in case the attacker gains access of the hypervisor all the data of the virtual machine including the kernel states as well as the inputs from the keyboard will be compromised.

Data plane attack: During the process of live migration, xen doesn't encrypt the migration data like the memory states of the virtual machine, dirty pages etc. and any third party can monitor the network used for transmission to access the sensible information and even launch active attacks on the virtual machine.

Migration module attack: Also the migration module protocols are transmitted as clear text and the attacker can sniff into the network and inject some malicious code into the module to subvert the migration process.

3.2. Virtualbox

Control plane attack: Without proper access control rules, any node in the data centre can emerge as an attacker. Since many initiators use the same shared storage which is a compulsion for the live migration to take place, control plane attacks can be performed.

Data plane attack: When teleporting a machine, the data stream through which the machine's memory contents are transferred from one host to another is not encrypted. A third party with access to the network through which the data is transferred could therefore intercept that data[7].

3.3. HyperV

Control plane attack: If Hyper-V servers don't belong to the common active directory forest, CredSSP based authentication is used which works by passing credentials to a remote computer to complete the authentication. If the remote system is compromised, then the credentials as well as live migration will be compromised.

4. Possible Control Plane Attacks

4.1. Denial of Service Attack

The target machine is saturated with a large number of sham migration requests from the attacker physical machine to avert it from responding to legitimate migration requests in the given time span. Platform: Xen, Virtualbox, Hyper-V

4.2. Migration of Corrupted VM to legitimate Host

By initiating unauthorized outgoing migrations, an attacker may cause guest VMs to be live migrated to the legitimate machine and gain full control over the host. Due to inter VM communication, if access policies are not defined for controlled communication, a malicious VM can attack other VM running on the target machine to which guest VM was migrated. Platform: Xen, Virtualbox, Hyper-V

4.3. VM Diversify

By initiating unauthorized incoming migrations, an attacker may cause guest VMs to be live migrated to the attacker’s machine and gain full control over guest VMs. Platform: Xen, Virtualbox, Hyper-V

5. Possible Data Plane Attacks

5.1. Information Leakage

By monitoring the migration path and network stream, the attacker can do this passive attack and extract sensible information from the memory of vm which is being migrated. Platform: Xen, Virtualbox

5.2. Man in Middle Attack

An attacker tries to include some malicious information into on-going conversation between sender and receiver and to have knowledge of the important data transferred between them. Platform: Xen, Virtualbox

6. Possible Attacks on Migration Module

6.1. Software vulnerabilities

The attacker can compromise the vm migration by using software vulnerabilities like stack overflow, heap overflow and integer overflow to inject malicious code into the migration module. Platform: Xen

6.2. Replay attack

Since the control messages of live migration protocols are sent unprotected, the attacker can access the credentials and replay the process of migration to by sending it’s vm to the host. Platform: Xen

6.3. Masquerading

After having access to the credentials of the machines, the attacker may modify the migration module to suspend the ongoing migrating process and send it’s own vm impersonating to be the original source. Platform: Xen

Table 1 List of possible attacks on various platforms

Plane	Attack	Platform
Control plane	Denial of service	Xen, Virtualbox, Hyper-V
	False resource advertising	Xen, Virtualbox, Hyper-v
	Migrating corrupted VM to legitimate host	Xen, Virtualbox, Hyper-v
	VM diversify	Xen, Virtualbox
Data plane	Man in the middle attack	Xen, Virtualbox
	Information leakage	Xen, Virtualbox
Migration module	Software vulnerabilities	Xen
	Replay Attacks	
	Masquerading	

7. Conclusion

In this paper, we systematically investigate the possible attacks to various cloud platforms. The goal of this research is to ensure functional correctness and security for cloud computing infrastructure. To achieve that it is necessary to analyze the security attacks and then it is required to help the developers to come up with secured integrated solutions.

References

1. Yuki Ashino and Masayuki Nakae, "Virtual Machine Migration Method between Different Hypervisor Implementations and its Evaluation", 26th International Conference on Advanced Information Networking and Applications Workshops, 2012.
2. Y Saeed Al-Haj and Ehab Al-Shaer, "A Formal Approach for Virtual Machine Migration Planning", 9th IEEE CSNM, 2014.
3. Zahra Tavakoli et al., "A Framework for Security Context Migration in a Firewall Secured Virtual Machine Environment", In the IFIP, LNCS Vol. 7479, 2013.
4. Jon Oberheide et al., "Empirical Exploitation of Live Virtual Machine Migration", In the Proc. of BlackHat DC convention, 2008.
5. Y Jarraya et al., "Cloud calculus: Security verification in elastic cloud computing platform", In the Proc. International Conference on Collaboration Technologies and Systems (CTS), 2012.
6. Michael Pearce et al., “Virtualization: Issues, security threats, and solutions”, ACM Computing Surveys (CSUR), Volume 45 Issue 2, February 2013.
7. www.virtualbox.org