Secure Live Virtual Machine Migration through Runtime Monitors

Ahmed M. Mahfouz, Md Lutfar Rahman, Sajjan G. Shiva
Department of Computer Science
The University of Memphis
Memphis, TN, USA
amahfouz@memphis.edu; mrahman9@memphis.edu; sshiva@memphis.edu

***Abstract*— In this paper, we propose a new model for live migration of virtual machines (VMs) in a secure environment. The live migration of a VM is the process of moving the VM from one physical host to another without interrupting any of the VM running services. We review the stages of the live migration process and identify the threats to it. Also, we propose our migration model that fulfills the most security requirements for secure live VM migration process.**

***Keywords*— Runtime monitor; Virtual Machine; Live migration; virtualization; Hypervisor.**

I. Introduction

Cloud computing has seen an enormous evolution in recent years. It has acquired popularity in the information technology (IT) world due to its efficiency in transferring capital expenditure to operational expenditure [1]. Cloud consumers can get access to a high-end computing infrastructure of clouds by only paying for their usage duration. Other advantages of cloud computing include: broad network access, on-demand self-service, resource pooling and rapid elasticity [2]. However, cloud computing has also brought some new vulnerabilities in addition to the existing security threats in the traditional IT systems. The security concerns of cloud systems are divided among three parties: the cloud vendors, the cloud users and the third-party vendor involved in ensuring secure sensitive software or configurations. If application level security is the responsibility of the cloud user, the provider is responsible for the physical security and also for enforcing external firewall policies. Security for intermediate layers of the software stack is shared between the user and the operator. Our goal in this paper is to focus on the security measures that are taken by the service providers to ensure the protection of customer data, application security and service availability. Cloud service providers (CSPs) have become increasingly active in implementing aggressive measures to address the security concerns of their customers. They have implemented several types of intrusion detection systems (IDSs) on high-volume networks to monitor different activities in order to detect potential malicious activities, intrusions, or policy violations. The recent 'dirty dozen' report from Cloud Security Alliance (CSA) [3] identifies twelve prominent threats to cloud systems: data breaches, compromised credentials, broken authentication, exploited system vulnerabilities, hacked interfaces and APIs, malicious insiders, account hijacking, advanced persistent parasites threats (APTs), inadequate diligence, permanent data loss due to provider error, cloud service abuses, denial of service (DoS) attacks and shared technology dangers.

In this paper, we propose the use of real-time monitors, which are programs for monitoring critical aspects of the application modules during the execution at various levels to detect and prevent different hacking attacks.

II. Moving Target Defense

IT systems are built to operate on static environment. This static nature gives the attacker sufficient time to study the system. Then the attack can be performed in adequate time so that it can goes unnoticed. Attackers maintain back doors without being discovered for long period of time [4]. To overcome these situations, a new defense strategy known as Moving Target Defense (MTD) has been adopted in IT. The concept came from battle field defense. In a battle field, the technique is to change resource positions so that the enemies get confused and find it difficult to attack. Similarly, if the target system is moved in an IT system, the uncertainty and complexity for the attackers will increase.

There are a number of different techniques and strategies used in moving target defense that are discussed in [5]

III. Live Migration

Live migration of VM requires the transfer of the complete state of a VM from source host to destination host. The complete state comprises all the resources that the VM uses in the source host. These resources include volatile storage, permanent storage, internal state of the virtual CPUs, and connected devices (e.g. LAN Cards). Meanwhile, the network-attached storage provides the permanent storage in the data center; hence, it is not required to move the permanent storage during the migration of VM. The internal states of the virtual CPUs are only a few kilobytes of data, so it does not take a considerable amount of time to be transferred. Longer periods are required to transfer the volatile memory contents which affect the performance of the live migration process. More attention is given therefor to improve the transfer of volatile memory from the source to the destination. The live migration process involves four main stages:

1. *Setup stage:* This stage involves selecting the migrated VM along with destination physical platform. It also involves setting up a transfer control protocol (TCP) connection to migrate VM's configuration data between the source and the destination platforms.

Finally, during this stage the memory is allocated and the skeleton of the VM is set up on the destination physical host.

2. *Memory transfer stage:* In this stage, the memory of the migrated VM is pre-copied to the new allocated memory on the destination host.
3. *Storage transfer stage:* During this stage, an up-to-date copy of the virtual hard disks files is being transferred from the source physical host to the destination physical host.
4. *Network clean-up stage:* This last stage of live migration involves updating all network switches to make sure that all the connections that were opened before the migration remain opened after the migration.

The performance of live migration of VM is measured by four metrics. They are as follows:

1. *Downtime:* This denotes the period during which the VM is completely shut down.
2. *Total migration time:* This is the period between the start of live migration until the resource of the source host are released.
3. *Time-to-responsiveness:* This represents the time span after the resume phase has ended until the VM achieves a certain guaranteed minimal utilization.
4. *Amount of transferred data:* This measure the amount of data received at the destination host from the different sources.

IV. Threats to Live Migrations

Live migration in cloud computing is vulnerable to a lot of active and passive attacks, such as false resource advertising, DoS, passive snooping, etc. [6, 7]. Attacks on live VM migration are categorized into three main classes:

A. Control Plane class

All server operations, including initiation and management of live migration, defining VM's setting, termination of a running VM, etc., should have an adequate authentication to secure the migration process against potential attacks. Failure to secure the control plane may allow unauthorized users to attack the live migration process in different ways [8]. Some of the possible attacks at the control panel include:

- *Control of Incoming Migration:* Unauthorized incoming migration may be initiated which may allow the attacker to live migrate guest VM to his server and hence gain a full control of the VM.
- *Control of Outgoing Migration:* This form of attack allows the attacker to live migrate a lot of guest VMs to a legitimate VM for no reason other than making the host OS overloaded, resulting in a denial of service.
- *False Resource Advertising:* The attacker may influence the control plane to live migrate VMs to a compromised virtual machine manager (VMM) by falsely advertising available resources. For example, the attacker may pretend that he has a substantial number of additional CPU cycles [9].
- *Disrupt regular operations of VMs:* For this type of attack on control plane class, the attacker may live migrate VMs between hosts to interrupt the operations of the VMs [8].

B. Data Plane Class

The data plane across which VM migrations occurs might be compromised to snooping and tampering [10]. Various techniques such as DNS poisoning, route hijacking, and ARP spoofing could help the attacker to be capable of logically positioning himself in the migration transit pass. That gives access to the confidential information that is being transferred during migration process. Threats and vulnerabilities on data plane are identified as following:

- Passive Snooping: An attacker may use several sniffing tools to observe the transmission channel and associated network stream. With these tools, the attacker may be able to extract confidential information from the migrated VM's memory such as passwords, keys, application data, and other protected resources.
- Active Manipulation: A type of the "Man in The Middle" attack, where the attacker can manipulate the memory of the migrated VM while being transferred across the network. This may result in a complete and hidden compromise of the guest OS [10].

C. Migration Module Class

The migration module is the software component responsible for all migration related functionality. Vulnerabilities in this module may enable the attacker to compromise the hypervisor component and subvert the VMM. If the attacker can compromise the hypervisor, the integrity of any guest VM running within the hypervisor and any VM that is migrated to that hypervisor in the future will also become compromised. Hammad and AlOazzaz [7] noted that stack overflow due to integer signedness issue and heap overflow due to issue in memory allotment routine are some of the vulnerabilities the attackers may use.

V. Requirements for Secure live VM Migration

The following security requirements are recommended by [11-13] for VMs migration processes:

- *Platform Integrity Verification:* for trust establishment, the destination platform should cryptographically identify itself to the source platform.
- *Authentication:* to avoid the "Man in The Middle" attacks; both source and destination hosts should mutually authenticate each other.
- *Authorization:* To prevent all unauthorized activities by applying appropriate access control policies.
- *VMs Confidentiality and Integrity during the migration process:* This type of security requirement is carried out by establishing an encrypted channel, which will

prevent an attacker from getting information from VM contents. This therefore helps to prevent active attacks.

- *Replay Resistance:* the process of live VM migration should be replay resistant to avoid making the attacker an authenticated user by capturing the traffic and replaying it later.

VI. Related Work

Several solutions have been proposed and implemented to avoid attacks on live migration. In this section, we present some of the proposed solutions in literature.

A. Isolating Migration Network:

The idea is to do the live migration in a completely separate network. In this way, the outsiders will have no clue that migration is going on (Fig. 1). Openstack is a good example of this technique.

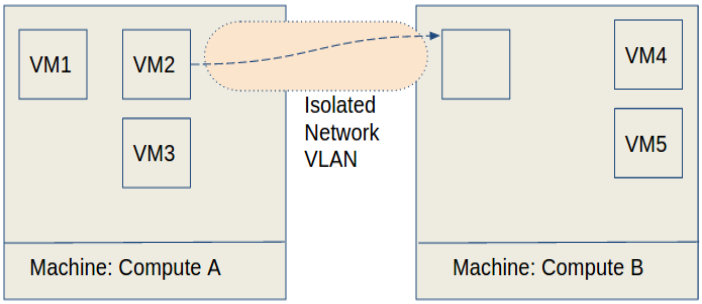

Fig. 1. Isolated network for migration.

B. Network Security Engine Hypervisor(NSE-H):

Hypervisor is a "Meta" operating system in a virtual environment. It has access to all physical devices. VMs access all the resources through Hypervisor [14].

There are two types of Hypervisor:

a. Hypervisor that operates on top of OS.

b. Hypervisor that directly operates on top of Hardware.

NSE-H implements some extra functionalities like firewall, IDS or Intrusion Prevention System (IPS) in the hypervisor (Fig. 2).

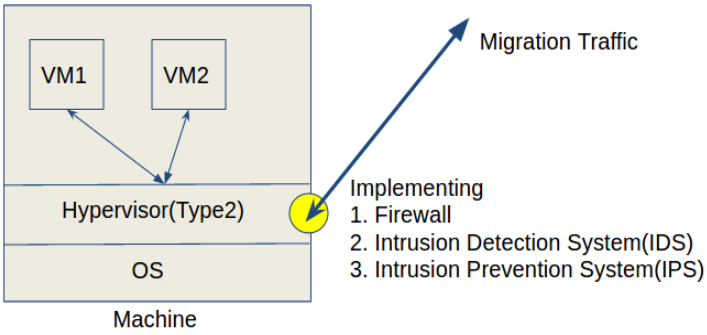

Fig. 2. Firewall in Hypervisor.

C. Secure VM-vTPM Migration Protocol:

Virtual Trusted Platform Module (vTPM) can be implemented if the hardware has the Trusted Platform Module (TPM) support. It offers a secure authentication protocol for the migration traffic [15]. In this protocol, the source and destination machine authenticate, attest and check the integrity of the connection before the migration. Then, it securely performs the encrypted migration (Fig. 3).

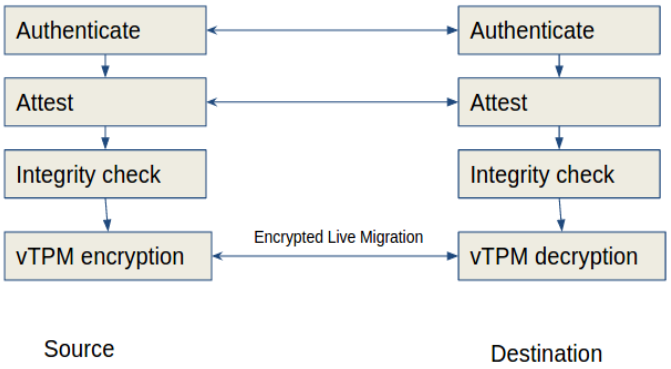

Fig. 3. Firewall in Hypervisor.

D. Improved VM-vTPM Migration Protocol:

This improved version of vTPM protocol adds an extra layer in the protocol. This extra layer is called Diffie Hellman (DH) key exchange.

E. Using SSH Tunneling:

The purpose is to hide the details of the source VM and the destination VM.

F. IPSec Tunnel:

Internet Protocol Security (IPSec) is a secure protocol in network layer that is used for securing the IP traffic. It proposes that the migration traffic should be encrypted as a normal IP packet [16]. The problem with this approach is that it slows down the migration process resulting in increased live migration down time (Fig. 4).

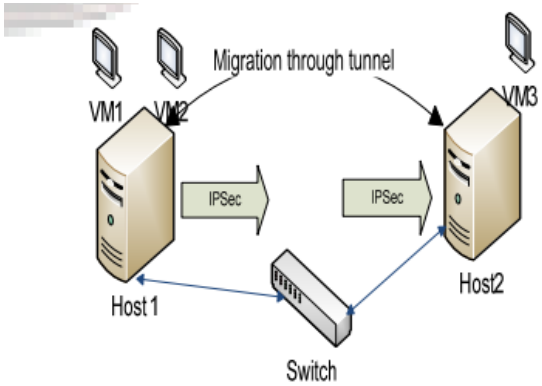

Fig. 4. Migration through IPSec tunneling.

VII. PROPOSED SOLUTION

A. Runtime Monitors for Live Migration

In our proposed model, we suggest involving monitors for all migration activities in the VM live migration process. Thus, for every hypervisor or guest VM we will add an independent monitor agent. The role of the agent is to monitor different processes and find any anomalous activity.

The model architecture includes three main components:

1. *Control Manager:* it is the heart of our model that receives migration requests from different hypervisors. It also issues agents to monitor all migration processes and has the authority to suspend or terminate any migration process. No VM migration process will start without permission from the control manager.
2. *Monitor Agents:* an agent is a "Monitor" that has the role of monitoring the migration process and reports any anomaly to the control manager. If any disputed activity is found, the control manager will immediately interfere, investigate, and if needed terminate the process. This model includes two types of agents:
    - VM dedicated agent: an agent with an intrusion detection system that monitors all migration activities of a specific migrated VM.
    - Attack dedicated agent: an independent monitor agent that is dedicated for monitoring the whole network for a specific type of threats on live migration e.g. DoS attack.
3. *Database Module (DBM):* A database contains information about all hypervisors and guest VMs. Any new installed hypervisor must have a record that includes all its information in this database, for example, IP and MAC addresses. New hypervisors can be added only by users with admin privileges.

During the migration setup stage and before setting up a TCP connection between the source and the destination hosts, the source hypervisor sends a migration request to the control manager. The migration request includes information about source and destination platforms to be used in the authentication process. The authentication process involves three steps: authenticating both platforms, calculating the load on the destination platform to decide whether it can accept new migrated VM without affecting the other hosted VMs, and creating new record for the new VM in the database.

Once the authentication process has been completed successfully, an encrypted TCP channel will be established between the two hosts and an agent will be dedicated to monitor the migration process. The agent will have all required information to monitor the migration process as well as a unique time stamp nounce.

During the migration process, many agents will be monitoring the entire network for specific threats and a dedicated agent will be assigned to monitor each migrated VM activities.

B. Security Analysis

Our proposed model can prevent many types of threats or attacks that might happen during the live VM migration process.

- *Control plan attacks:* during the authentication process, the control manager will prevent attackers from initiating unauthorized migration or overuse the resources of legitimate VMs. This prevents the incoming and the outgoing migration control attacks. Also, by authenticating the destination platform, VMs will be migrated only to healthy trusted platforms which prevent any false resource advertisement attack.
- *Data plan attacks:* any anomaly will be reported directly to the control manager by using an encrypted communication channel monitored by an agent with IDS. The control manager will take the proper action to prevent passive snooping, active manipulating, and "Man in The Middle" attacks.
- *Migration module attacks:* The migration module provides the network service over which a VM is transferred [13]. Our model includes an agent with IDS to monitor these services. The agent will report any discovered vulnerability to the control manager that can take the required action to prevent any possible attack.

C. Top-level attack scenario

A DoS attack may take one of the following two scenarios:

- An attacker may insert automated migration script in the controller machine. In an infinite loop the script will try to live migrate all the listed VMs to other legitimate machines. All the VMs will start moving at a time and the network will be flooded with so many copies going on and VMs never get the chance to stabilize. The end result is that all VMs will be unavailable to the outer world.
- The attacker may capture traffic and replay it many times which will overload the destination host and cause disruptions.

D. Defense using the proposed solution

Beside the VMs agents, there will be one agent dedicated for detecting DoS attacks on live migration by constantly checking the number of migrations happening at a moment. If the number exceeds a specific threshold, then it will suspect DoS attack and report it to the control manager. Also, when the attacker tries to replay any captured traffic, the control manager will check the time stamp nounce and prevent this new.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we have discussed the live VM migration and its security threats. We have demonstrated some of previously proposed solution for such threats. Also, we proposed a new security model which overcomes most attacks during the live migration processes. Our model is based on using runtime monitor agents to report any threats to a control manager, which has the authority to suspend the attacks. As a top-level attack scenario, we have showed how the new proposed model

can prevent a DoS attack. The model implementation and complexity evaluation have been left for the future work.

REFERENCES

[1] Srinivasan, S. Building trust in cloud computing: Challenges in the midst of out ages. Proceedings of Informing Science & IT Education Conference (InSITE), pp. 305-312, 2014.

[2] Mell, P., & Grance, T. The NIST definition of cloud computing. National Institute of Standards and Technology Special Publication, 2011.

[3] Rashid, F. The Dirty Dozen: 12 Cloud Security Threats, Infoworld, 2016.

[4] Zhuang, Rui, Scott A. DeLoach, and Xinming Ou. A model for analyzing the effect of moving target defenses on enterprise networks. In Proceedings of the 9th Annual, 2014.

[5] Xu, J., Guo, P., Zhao, M., Erbacher, R. F., Zhu, M., & Liu, P. Comparing Different Moving Target Defense Techniques. In Proceedings of the First ACM Workshop on Moving Target Defense, pp. 97-107, 2014.

[6] Tanvi Pandya, Madhuri Bhavsar, Live Migration in Cloud and its Security Concerns: A Survey. IJCSC, 6(1), pp.62-66, 2015.

[7] Hatem M. Hamad, Alaaeddin B. AlQazzaz, Secure Live Virtual Machine Migration by Proposed Security Center, IUGNES, 24(1), pp 14-20, 2016.

[8] Alshahrani, Hani, et al. Live Migration of Virtual Machine in Cloud: Survey of Issues and Solutions. In proceedings of the International Conference on Security and Management (SAM), 2016.

[9] Sharath Venkatesha, Shatrugna Sadhu, Sridhar Kintali. Survey of Virtual Machine Migration Techniques, Department of Computer Science, University of California, 2009.

[10] Jon Oberheide, Evan Cooke, Farnam Jahanian. Empirical Exploitation of Live Virtual Machine Migration. Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI 48109, 2007.

[11] Shetty, J., Anala, M. R, Shobha, G. A Survey on Techniques of Secure Live Migration of Virtual Machine. International Journal of Computer Applications, 39(12), 2012.

[12] Abuhussein, S. Shiva, F. Sheldon, CSSR: Cloud Services Security Recommender, IEEE 11th World Congress on Services (SERVICES) - Emerging Technology Track: Dependable and Secure Services (DSS 2016), San Francisco, California, 2016.

[13] Abuhussein, F. Alsubaei, S. Shiva, F. Sheldon, Evaluating Security and Privacy in Cloud Services, IEEE NATA-COMPSAC Symposium on Novel Applications and Technology Advances in Computing, the 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, Georgia, June 2016.

[14] Xianqin, C., Han, W., Sumei, W., Xiang, L.: Seamless virtual machine live migration on network security enhanced hypervisor. In Procceding of IEEE International Conference on Broadband Network and Multimedia Technology, pp. 847---853. IEEE (2009).

[15] Fan, P., Zhao, B., Shi, Y. et al. Wuhan Univ. J. Nat. Sci. 20: 512., 2015.

[16] Anupam Tamrakar, Security in Live Migration of Virtual Machine with Automated Load Balancing, International Journal of Engineering Research & Technology (IJERT), 3(12), 2014.

`