Live Migration using VM/TPM Protocol of Virtual Machine on Private Cloud

Vaishakhi Maheshwari¹, Prof. Mohit Patel²

¹Department of Computer Engineering, Swaminarayan College of Engineering and Technology, Kalol, GTU, India
²Department of Computer Engineering, Swaminarayan College of Engineering and Technology, Kalol, GTU, India

¹vaishakhimaheshwari@gmail.com, ²patelmohit9932@gmail.com

Abstract—Cloud computing means storing and accessing data and programs over the internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet. The on premises private cloud demands the security on data expansion. The concept of virtualization plays a vital role in providing secure cloud computing. The virtual machines which are emulation of a computer system over the cloud are combination of hardware and software. For achieving energy efficiency, load balancing and high availability of physical server in Cloud Data Center, the virtual machines should be migrated from one physical server to another. The migration process is not reliable until it provides security to the transferring data over the cloud. For this purpose VM-vTPM protocols can be used. vTPM should be migrated to the desired platform together with its corresponding virtual machine. Only vTPM are not secure enough so VM-vTPM comes forward to solve these issues. In this paper, we focus on the secure implementation of virtual machine migration from one platform to another platform in private cloud model. We propose a thorough and secure VM-vTPM migration scheme. In this scheme we first propose a vTPM key structure to make non-movable vTPM keys to be sent. Then we depend on this structure to construct a secure VM-vTPM migration protocol which includes three phases. The first phase is a dual authentication between source platform and destination platform, the second phase is the migration of vTPM, and the third phase is the migration of VM. Finally, we analyze the security of our protocol to make sure our proposed protocol can realize all the security goals such as confidentiality and integrity, authentication of source and destination platform, preserving the association between VM and vTPM, and atomicity of the transfer.


I. INTRODUCTION

Cloud computing is provides A u means by which we can access the application as utilities over the Internet. It allows creating, configuring and customizing application online. Cloud can provide over the Internet. Cloud providing to run applications such as email, web conferring, and customer relationship management. Virtualization is the techniques which divides physical machine into several completely isolated machine known as virtual machine.
II. Virtualization

Virtualization is the abstraction and emulation of hardware resources to have better resource sharing. The server Virtualization is the ability to run multiple virtual machine, including their operating system called Guest operating system or existing real operating system called Host operating system.[2]

Many physical servers that connected by a physical switch, IT department get collected information about the traffic that transmit between servers from physical switch. That means it does not provided a virtual switch result lack of visibility into the traffic flows between among the VMs on the same physical level that impact security performances.

(A) Live Migration

Live VM migration is best characteristics of virtualization defined as process of dynamically transferring running VMs from one physical server to another with little or zero downtime and without interrupting services running in VM.[2] Live migration is the movement of virtual machine from one physical host to another while continues power up.

Live Migration process can be described below:[1]

Push phase: The source VM continues running while certain pages are pushed across the network to destination

Stop and copy phase: The source VM is stopped, pages are copied across to the destination VM, then the new VM is started downtime of a VM during a Live migration could be a few millisecond to seconds according to the size of memory and application running on the VM.

Pull phase: The new VM executes and, if it accesses a page that has not yet been copied, this page is pulled.

(B) Security Analysis

Different types of security described below:

Integrity Verification

Client’s platform integrity and to needs to be analyzed by remote host and to secure client’s platform integrity measurement from any illegitimate parties and this done by encrypting the measurement with session key (k). The integrity measurement value, attacker would need to capture (k) it is impossible as (k) has never been exchanged between clients and server. Therefore uses TPM as tamper proof hardware that protect all the measurements from manipulate of client’s side.

Impersonation Attack

As Implementations of SRP Protocols requires zero knowledge proof without session key (k) attacker would not able to compute evidence Mc or Ms, moreover session key is never passed over the network and this will make Impersonation attack almost Impossible.

Stolen Verifier Attack

The Strength of the proposed is that even though attacker manages to steal the verifies (v), the attacker would not able to continue with authentication process without client’s password as it requires expensive dictionary search to reveal it.

Insider Attack

The Strength of our proposed protocol is that it does not store any client’s password or server secret key in the server side. Therefore our scheme can prevent the insider from stealing sensitive authentication information.

Identity Protection

The proposed preserves user identity privacy by replacing user identity with pseudonym identity (u).which is a hashed value of user identity and selected platform PCR values. Pseudonym identity is important because in the event of server’s database has been compromised: user identity privacy is still protected due to the fact that attacker cannot manipulate the pseudonym identity or link it back to actual user.

III. LITERATURE SURVEY

Virtual trusted platform module (vTPM) provides trusted computing for multiple virtual machine (VM) running on single platform. Trust platform module provides hardware and software support for secure storage and software integrity protection. virtualized computing systems enables the hardware based protection of private information and the detection of malicious software that aims the break the operation of virtualization environment.

- Requirements for secure VM-vTPM Migration Protocols[6] :-

This research paper identified and formulated security requirement that should be provided for secure VM-vTPM Migration protocol.
The result for research with security as follows:

A) **Authentication of transfer platforms**: An attacker must not be able to launch MITM (man in the middle) attacks or bait and switch attacks. The attacker must not be able to migrate a vTPM from a secure platform to his insecure platform or vice-versa.

B) **Confidentiality and integrity of data transfer**: An untrusted entity should not be able to learn any meaningful full information about the VM-vTPM during the migration process and should not be able to modify the vTPM without the modification being detected.

C) **Replay resistance**: An attacker should not be able to replay an old communication sequence successfully without the reply being detected.

D) **Source non-repudiation**: It must not be possible for the source to deny the migration.

E) **Atomicity of the transfer**: Ensure deletion at the source in case of successful transfer and deletion at the destination in case of failure are required to ensure atomicity of the migration. It is critical for failure recovery and to prevent duplicate copy generation.

- **Designs for vTPM Migration Protocol**

  **Protocol outline**: In this section, we describe the vTPM-VM live migration process authenticity, of the communication, credibility of partners and confidentiality of transfer data, it is important to establish an authenticated channel between the source and destination.

  ![](image)

  **Phase 1: Establish trusted tunnel**
  - Initially, source and destination authenticate each other. The source sends a property based attestation request to the destination to ensure that vTPM migrated to a secure platform conformed to the security policy they negotiate security parameters and finally, they compute session key and exchange the handle of the session key for protecting the confidentiality of the rest of the transfer process.

  **Phase 2: Data transfer**
  - The source sends a request to migrate the vTPM and the destination responds with the migration parameters. The source then proceeds to create a secure channel and transfer the vTPM data in a secure manner. Finally, the destination deletes the vTPM to ensure atomicity of the migration.

Our vTPM migration protocol is based on the vTPM architecture. The migration process is divided into two phases: establishment of trusted channel and secure data transfer. Fig. shows the outline of vTPM-VM live migration process. The description of the two phases is summarized as follows:

**Phase 1: Establishment of trusted channel, initially**, source and destination authenticate each other. The source sends a property based attestation request to the destination to ensure that vTPM migrated to a secure platform conformed to the security policy they negotiate security parameters and finally, they compute session key and exchange the handle of the session key for protecting the confidentiality of the rest of the transfer process.
**Phase 2 Secure data transfer.** The source forward request to migration message to destination. Next the destination creates an empty vTPM instance for the purpose of migrating state and responses request. The source then locks the VM and vTPM and transfer the state data of vTPM securely. Then after destination check the integrity of the received vTPM state packages. If no violation are detected, on the target the vTPM decrypts the state packages and activation and sends an acknowledgement to the source on success. Finally, the source deletes the migrated vTPM to prevent duplication.

**IV. PROPOSED ALGORITHM AND IMPLEMENTATION STRATEGY**

We are proposing verification based on integrity here a new encryption scheme will be provided that enhances the security by prevention malicious virtual machine from damaging the live migration process. We assume that source and destination is on the same cloud and want to follow the secure channel provided by the platform far as attack. When VM talks to each other, it has possibility of attack in between and through message. Communication attacks between host/os and guest VM.

(A) PROPOSED ALGORITHM

**Step 1:** Start
**Step 2:** Launch VM
**Step 3:** Launch vTPM
**Step 4:** Setup USER
**Step 5:** Create & Launch instance
**Step 6:** Get Instance Key
**Step 7:** Generate metadata
**Step 8:** Integrity check (Hashing Technique)
**Step 9:** if checked set encryption
**Step 10:** Generate Encrypt Key
**Step 11:** Check Key
**Step 12:** Set and Match Key (decrypt)
**Step 13:** Unlock and Unpack message

(B) FLOW CHART

![Flowchart](image_url)
V. EXPECTED RESULTS

D(SH, C) – m.
Decrypt cipher text message m.
Cipher text and public key alone reveal nothing about message.

Comparison of latency of migration over cloud.

<table>
<thead>
<tr>
<th>No. of properties</th>
<th>10</th>
<th>20</th>
<th>30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer</td>
<td>0.7</td>
<td>0.5</td>
<td>0.8</td>
</tr>
<tr>
<td>Attestation</td>
<td>0.7</td>
<td>1.5</td>
<td>1.0</td>
</tr>
</tbody>
</table>

TABLE 1. Comparison Table

Here, latency means period of delay when one component of network is waiting for an action to be executed by another component.
Here, it’s the time required online or in a network for one way or round trip transfer of data between two nodes.

VI. CONCLUSION AND FUTURE WORK

Live VM migration is a useful feature but it is not reliable until it provides security to the transferring data over the cloud. In this paper, we focus on the secure implementation of virtual machine migration from one platform to another platform in private cloud model. We propose a thorough and secure VM-vTPM migration scheme. In this scheme we first propose a vTPM key structure to make non-movable vTPM keys to be sent. My feature work is to implement the proposed vTPM migration process on simulator and check its efficiency and security. My feature work is to implement the proposed vTPM migration process on simulator and check its efficiency and security.

REFERENCES


