2014 28th International Conference on Advanced Information Networking and Applications Workshops

Secure Live Virtual Machines Migration: Issues and Solutions

Mahdi Aiash, Glenford Mapp, Orhan Gemikonakli
School of Science and Technology
Middlesex University, UK
Email:{M.Aiash, G.Mapp, O.Gemikonakli}@mdx.ac.uk

***Abstract*—In recent years, there has been a huge trend towards running network intensive applications, such as Internet servers and Cloud-based service in virtual environment, where multiple virtual machines (VMs) running on the same machine share the machine's physical and network resources. In such environment, the virtual machine monitor (VMM) virtualizes the machine's resources in terms of CPU, memory, storage, network and I/O devices to allow multiple operating systems running in different VMs to operate and access the network concurrently. A key feature of virtualization is live migration (LM) that allows transfer of virtual machine from one physical server to another without interrupting the services running in virtual machine. Live migration facilitates workload balancing, fault tolerance, online system maintenance, consolidation of virtual machines etc. However, live migration is still in an early stage of implementation and its security is yet to be evaluated. The security concern of live migration is a major factor for its adoption by the IT industry. Therefore, this paper uses the X.805 security standard to investigate attacks on live virtual machine migration. The analysis highlights the main source of threats and suggests approaches to tackle them. The paper also surveys and compares different proposals in the literature to secure the live migration.**

I. Introduction

Among the leading business challenges confronting IT managers today are: cost-effective utilization of IT infrastructure; responsiveness in supporting new business initiatives; and flexibility in adapting to organizational changes. Driving an additional sense of urgency is the continued climate of IT budget constraints and more stringent regulatory requirements. Virtualization is a fundamental technological innovation that allows skilled IT managers to deploy creative solutions to such business challenges [1]. The term virtualization broadly describes the separation of a resource or request for a service from the underlying physical delivery of that service. With virtual memory, for example, computer software gains access to more memory than is physically installed. Similarly, virtualization techniques can be applied to other IT infrastructure layers - including networks, storage, laptop or server hardware, operating systems and applications. This blend of virtualization technologies - or virtual infrastructure-provides a layer of abstraction between computing, storage and networking hardware, and the applications running on it. The deployment of virtual infrastructure is non-disruptive, since the user experiences are largely unchanged. However, virtual infrastructure gives administrators the advantage of managing pooled resources across the enterprise, allowing IT managers to be more responsive to dynamic organizational needs and to better leverage infrastructure investments.

One main benefit allowed by virtualization: that of the live VM migration (LM) [2] [3] [4]. Migrating an entire VM and all of its applications as one unit allows us to avoid many of the difficulties faced by process-level migration approaches. In particular the narrow interface between a virtualized VM and the Virtual Machine Monitor (VMM), also known as hypervisor makes it easy to avoid the problem of 'residual dependencies' in which the original host machine must remain available and network-accessible in order to service certain system calls or even memory accesses on behalf of migrated processes. With virtual machine migration, on the other hand, the original host may be decommissioned once migration has completed. This is particularly valuable when migration is occurring in order to allow maintenance of the original host. Secondly, migrating at the level of an entire virtual machine means that in-memory state can be transferred in a consistent and efficient fashion. This applies to kernel-internal state (e.g. the TCP control block for a currently active connection) as well as application-level state, even when this is shared between multiple cooperating processes. In practical terms, for example, this means that we can migrate an on-line game server or streaming media server without requiring clients to reconnect. Thirdly, live migration of virtual machines allows a separation of concerns between the users and operator of a data center or cluster. Users have 'Carte Blanche' regarding the software and services they run within their virtual machine, and need not provide the operator with any OS-level access at all (e.g. a root login to quiesce processes or I/O prior to migration). Similarly the operator need not be concerned with the details of what is occurring within the virtual machine; instead they can simply migrate the entire operating system and its attendant processes as a single unit. Overall, live VM migration is a extremely powerful tool for cluster administrators, allowing separation of hardware and software considerations, and consolidating clustered hardware into a single coherent management domain. If a physical machine needs to be removed from service an administrator may migrate OS instances including the applications that they are running to alternative machine(s), freeing the original machine for maintenance. Similarly, VM instances may be rearranged across machines in a cluster to relieve load on congested hosts. In these situations the combination of virtualization and migration significantly improves manageability [3].

Most of the commercial and open source hypervisors now support live migration. However, the main focus was on the implementation of live migration with a little or no consideration towards its security [5]. Live migration might be susceptible to many attacks like "man-in-middle", "denial-

978-1-4799-2652-7/14 $31.00 © 2014 IEEE
DOI 10.1109/WAINA.2014.35

of-service" and "stackover flow" [6] [7] [8]. The data during the migration can be sniffed or tampered easily as it is not encrypted. Thus compromising integrity and confidentiality of migrating VM data. Due to these security concerns sectors such as healthcare, banking, business and national defence hesitate to take advantage of live migration. The current state of challenge is to develop mechanism to provide secure live migration of virtual machines. However, in order to develop an efficient security module, it is necessary to clearly identify the threats and risks of implementing LM. But since analysing security requirements of networking systems is quite complex, the ITU introduced a systematic analysis tool called X.805 [9] as a holistic approach to network security by discussing systems security requirements at different levels and pinpointing potential system vulnerabilities. The X805 architecture has been used to investigate the vulnerabilities of different systems such Asynchronous Transfer Mode (ATM) and 4G networks [10] [11]. Therefore, this paper uses the X.805 architecture to highlight the security threats of LM and then discusses some of the solutions proposed in the literature. The rest of the paper is organized as follows. Section 2 describes the procedure of live migration and gives an overview of the X.805 security architecture. A detailed security evaluation of live migration is given in Section 3 and a summary of the evaluation results is presented as well. Section 4 discusses a number of the proposed approaches in the literature to address security of live migration and compares between them. The paper concludes in Section 5.

II. Related Work

A. The Procedure of Live Migration

Virtual machine migration takes a running virtual machine and moves it from one physical machine to another. This migration must be transparent to the guest operating system, applications running on the operating system, and remote clients of the virtual machine. It should appear to all parties involved that the virtual machine did not change its location. Virtual machines provide a natural platform for migration by encapsulating all of the state of the hardware and software running within the virtual machine. There are three kinds of state that need to be dealt with when migrating a VM:

- The virtual device state including the state of the CPU, the motherboard, networking and storage adapters, floppy disks, and graphics adapters.
- External connections with devices including networking, USB devices, storage devices, and removable media such as CD-ROMs.
- The VM's physical memory.

Generally speaking, the actual migration process involves several steps:

1) **The Set up Stage:** It starts the migration process by selecting the VM to be migrated along with the destination host. It also sets up a TCP connection between the source and destination hosts to transfer the configuration data of the virtual machine. On the destination physical host, memory is allocated and a skeleton of the virtual machine is set up.
2) **The Memory Transfer Stage:** This stage involves pre-copying the memory state of the VM to the destination host while the VM is running on the source host.
3) **The Storage Transfer Stage:** In this stage, the control storage associated with the source physical server, such as virtual hard disks (VHD) files are transferred to the destination host. At the end of this stage, the destination host has an up-to-date virtual machine and access to any associated storage medium.
4) **The Network Clean-up Stage:** In order for a migration to be transparent, all network connections that were open before migration must remain open after migration completes. Since each VM will have Virtual Network Interface card (VNIC) which is identified by a MAC address, the VM needs to update the switches in the network so that the virtual machine traffic will be forwarded through the corresponding switch port.

B. An overview of the X805 architecture

As described in [9], the X.805 standard defines three security layers (applications, services and infrastructure), three security planes (end user, control and management) which are identified based on the activities performed over the network, and also eight security dimensions to address general system vulnerabilities (Access Control, Authentication, Non-Reputation, Data Confidentiality, Communication Security, Data Integrity, Availability, and Privacy) [9].

III. Live Migration Security Evaluation

A. Analysing the Security of Live Migration Using the X805 Architecture

In this section we apply the X.805 standard to analyse the security of LM. Since LM is an infrastructural procedure that enables running VMs to move between different physical hosts, the functionality of this procedure is only related to the Infrastructure Layer of the X.805 standard which is concerned with the security of network links and elements. As previously mentioned, each layer is decomposed into three planes (Table I), and for each plane eight vulnerabilities corresponding to the security dimensions of X.805 are examined. The management plane is represented as Module 1, the control plane is represented as Module 2 and the user plane is represented as Module 3, each vulnerability is analysed relative to Module 1, 2 and 3. In the context of Live Migration, the three security planes could be described as follows:

1) The Management Plane: The VMM that implements migration functionality must be resilient against attacks. If an attacker exploits a vulnerability in the VMM, he may gain complete control over both the VMM and any guest VMs [13].

2) The Control Plane: The communication mechanisms and models used by the VMM or hypervisor to initiate and manage the live migration must be authenticated and resistant to tampering.

3) The End-User Plane: This plane deals with providing end-users with a secure and authorized access to migrating VMs.

TABLE I. A GENERAL DEFINITION OF THE SECURITY PLANES IN THE X.805

The Security Plane	Description
The End-User Security Plane	Access and use of the network by the customers for various purposes such as basic connectivity, value-added services (VOIP, VPN, etc) and Access to network-based applications (e.g., email, file sharing)
The Control/Signaling Security Plane	Activities that enable efficient functioning of the network (Update of routing/switching tables and service initiation, control, and termination)
The Management Security Plane	The management and provisioning of network elements, services and applications. This plane involves all the functions defined in the fault, configuration, accounting, performance, security (FCAPS) management model.

Below, we discuss the eight security dimensions in the context of live migration.

1) **Access Control:** An inappropriate access control policy allows an unauthorized user to initiate, migrate and terminate a virtual machine. For instance, an unauthorized attacker can migrate a VM with malicious code to a legitimate target hypervisor. This provides a platform for the malicious VM to perform internal attacks on target system. For example gaining control over the target hypervisor and other guest VMs. Furthermore, since the VMs running on the same machine can communicate with each other, if access policies are not defined for controlled communication, a malicious VM can attack other VM running on same machine [12].
To prevent an attacker from performing such an unauthorized activities appropriate access control policies must be defined; access controls lists (ACLs) might be also implemented to enforce different levels of access rights i.e., on the physical hosting machine and VMs.
2) **Authentication:**
   - Module One: When a LM is initiated, there is a need for mutual trust and authentication between the source and target physical hosts. The authentication mechanisms can also be accompanied with a firewall to check that migration is from allowed source and to allowed destination systems.
   - Module Two: An untrusted, malicious VMs might initiate or terminates LM. For instance, in the case of Dynamic Load Balancing where live migration is automatically initiated from heavily loaded VMM to another less loaded one [12], a malicious VM might falsely advertise available resources (by claiming to have a large number of spare CPU cycles for instance) and hence, influence the migration policy to migrate the machine to a compromised target, where the attacker will control the migrated VM. Another possible scenario, is when a malicious end-user exploits this feature by overloading a server and creates large number of VMs such that the load balancing feature migrate one or more VMs to another host.
   - Module Three: The system administrator controls the operation of server through the management console. Normally system administrator is an authorized personnel with rights to perform crucial configuration and set-ups. Thus this interface can be a platform for attacks on virtual machine. The attacks can be deliberate attempts to impersonate the system administrator to gain access to the interface. In an enterprise environment, administrators with different roles like system administrator, security administrator, and network administrator will be defined. That is more persons will need to have the superuser/administrator privilege. This increases the security risk of compromising the whole system via the administrative interface [12]. Indeed, system administrator role is very important in preserving the security of the system; therefore, there is a need to implement a very strict authentication and identification procedures.
3) **Non-Repudiation:** There is a need for a monitoring and accounting the system's activities; hypervisors and end-users should be held accountable for their actions. When live migration takes place either manually by a system administrator or automatically via the Dynamic Load-Balancing feature, all relevant activities have to be audited in a secure logging system.
4) **Data Confidentiality:** The VM migration protocol does not encrypt the migration data nor the signalling/control messages by default. Thus the migration data appears as clear text over the network. To deal with this problem, there is a need to encrypt both the VM storage data as well as using encryption algorithm to secure the control messages of live migration protocol. This dimension is relevant to all three modules.
5) **Communication Security:** As described above, the insecure and unprotected transmission channel is result of the migration protocol. The migration protocol does not encrypt the data as it travels over the network, thus susceptible to active and 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 [15]. Passive attacks include eavesdropping of messages for sensitive data, passwords and keys, capturing authenticated packets and replying them later. Active attacks are more serious. For example manipulating authentication services like sshd, /bin/login [5]. To deal with this situation there is a need to define secure channels for migration traffic for example by using VPN tunnels between the source and target hosts. This threat has impacts on all three modules.
6) **Data Integrity:**
   - Module One: Vulnerabilities in migration module such as stack overflow, heap overflow and integer overflow can be exploited by an attacker to inject malicious code or even halt the LM process.

- Module Two: As described earlier, the control messages of the live migration protocols are sent unprotected, hence a malicious attacker might be able to manipulate the messages and launch replay attacks.
- Module Three: In addition to data integrity, the integrity of the physical host could be a main source of threat, as an attacker might migrate a victim VM to a compromised physical host and hence gains full control over the VM. This implies that all users and processes run on this VM will be exposed.

To address the integrity issue, it is strongly recommended to deploy the new release of virtualization software that includes patch of newly discovered vulnerabilities. The system must be updated with the recent releases and patches to be protected from such vulnerabilities. Also secure programming methods such as type safe language must be used. Other solutions include encryption of migration data to provide confidentiality; Integrity can be preserved using MAC, digital signatures and checksums [5].

7) **Availability:** An unauthorized attacker can initiate large number of outgoing migrations onto a legitimate virtualized host server. Thus overloading target server, decreasing its performance or at worst disrupting service it provides. Also it is possible for an unauthorized attacker to make the VM to migrate from server to another, reducing the performance of service provided by VM and generating huge volume of traffic that degrades the network performance. In order to mitigate such attacks there is a need for deploying a combination of security measures at all security planes. Examples of these measures are appropriate access control policies to stop unauthorized users and malicious VMs from gaining access. There is a need for implementing packet filtering techniques to check for allowed sources and targets hosts for LM. Authentication and auditing mechanisms are required as well for authentication and non-repudiation reasons.

8) **Privacy:**

- Module One: Running VMs can be live migrated without the knowledge of users who store their data within these VMs. While this transparency is an advantage to stop traffic analysis and tracking attacks [16], VMs might pass national borders during migration and internal data might become subject to different legislation or migrated to untrustworthy location.
- Module Two: A malicious user can migrate a malicious VM and place it on same host server as the target VM. The malicious VM then creates a covert-channel that leaks information of target VM [17].
- Module Three: A compromised VM or physical host might expose users' information and stored data to a third party without user consent.

One approach to secure live migration against all attacks discussed and preserved privacy is to assign a small group of VMs or even a single VM to its own host-based Virtual LAN (VLAN). VLAN [18] is basically a segmentation and isolation tool. The VLAN isolates migration traffic from other network traffic and defines a secure transmission channel for migration [19].

B. A Summary of the Analysis Results

The analysis in section III-A shows that several vulnerabilities are disclosed in the implementation of live migration. The major one is that the migration protocol does not encrypt migration data. All migration data i.e. kernel memory, application state, sensitive data such as passwords and keys etc are transmitted as clear text. Thus there is no confidentiality of transmitted data. Other vulnerabilities are migrating a VM to untrusted platforms, authentication and authorization of operations that control VM, integrity of VM data, bugs in hypervisor/migration module code etc.

Furthermore, the analysis shows that a secure live migration requires security to be applied before migration, during migration process, and after migration is done. Typically, a secure live migration requires:

- The source and destination physical hosts to be trusted.
- An authorized access to management interface; authenticated and authorized management capabilities (VM creation, deletion, migration etc) are in place.
- The migration data remains confidential and unmodified during the transmission.
- Protection against network attacks, intrusions and malicious codes.
- The presence of mechanisms to detect and report suspicious activities.
- Protection against vulnerabilities in the migration software.

IV. Solutions for Secure Live Migration

This section will discuss some of these proposals, highlight the pros and cons and compare them.

A. The CoM Security Framework

The authors in [20] proposed the CoM framework for a secure VM migration. The framework is based on hypervisors included with Network Security Engines (NSE) and hence the whole system is called Network Security Engine-Hypervisors (NSE-H). NSE includes firewall, intrusion detection systems (IDS) and intrusion prevention system (IPS) to provide security to virtualized environment and to eradicate intrusions occurring in virtual networks. The NSE firewall works in a state-full way and it includes built-in intelligent packet processing capabilities. The CoM framework enables the traditional security approaches like firewall, IDS, IPS present inside NSEs to work in context of live migration. It transfers the security context along with migration data so that the VM can be restored at the destination.

B. The Virtual TPM (vTPM) based solutions

Trusted computing is an approach to build systems such that their integrity can be verified [13]. It is based on the concept of transitive trust where initial trust in a hardware module is delegated to other system components. The industry standard trusted hardware module is the Trusted Platform Module (TPM) [21]. The authors in [22] identify the requirements for a virtual TPM (vTPM) and propose a vTPM design that supports running vTPMs in memory or on a cryptoprocessor. The architecture has been implemented on the Xen hypervisor [23]. Generally speaking, the vTPM migration protocol verifies the integrity of the source and destination hypervisors and establishes a secure connection between them before the live migration. It is worth pointing out that while this approach provides confidentiality, authentication and trust establishment it does not support live migration of VM; rather it supports migration of suspended VMs.

C. The Live Migration Defence Framework

When considering implementing live migration on a large scale such as in Cloud environment, it is important to keep in mind the fact that cloud providers like the Amazon EC2 maintain various data centers in different countries and they do not give precise information whether internal live migrations are used [14]. This means that running VMs can be live migrated without the knowledge of the owners who store their data within these VMs. It is also possible that the VMs pass national borders during a live migration, in which case the internal data can become subject to a different legislation. Furthermore, VMs can be manipulated during the live migration procedure or the new location can be untrustworthy. To address this problem, the Live Migration Defence Framework (LMDF) has been introduced in [14]. The LMDF detects a live migration in an early phase and delays an ongoing live migration to use the additional gained time to execute integrity and confidentiality measurements on internal data before migration. The framework aims at performing as much measurements as possible and transmits these values for later comparison before the live migration is finished. More details about the framework and implementation results can be found in [14].

D. Role-Based Migration Solutions

A number of solutions such as the one presented in [25] [12] adopt the role-based migration approach based on the use of Intel vPro and TPM hardware. The architecture of role-based live migration

establishes trust through attestation process, defines role-based migration policies. Thus it ensures only authorized user can perform migration operations, more details about the operation of the architecture are found in [25].

E. Security Analysis of the Solutions

As discussed in section III-B, for a secure live migration there is a need to meet a number of requirements. This section will discuss how efficient were the above discussed security solutions in meeting these requirements:

- **Requirement 1:** The source and destination physical hosts are trusted.
  - ○ The CoM Framework: Transferring the security context as part of the migration process will ensure mutual trust between the source and target hosts.
  - ○ The vTPM: This achieved using the TLS security protocol and destination attestation process.
  - ○ The LMDF: This is not achieved due to the absence of authentication and trust establishment mechanisms.
  - ○ The Role-Based Migration: This is achieved through the attestation process.
- **Requirement 2:** An authorized access to management interface.
  - ○ The CoM Framework: The deployment of firewall, IPs and IDs as part of the NSE-H will ensure the authorization of the migration process.
  - ○ The vTPM: No access control mechanism is in place to enforce authorized access.
  - ○ The LMDF: There is no access control mechanism.
  - ○ The Role-Based Migration: This is achieved using the Policy Service Module.
- **Requirement 3:** The migration data should remain confidential and unmodified during the transmission.
  - ○ The CoM Framework: This requirement is not achieved in this approach as data is not encrypted or hashed.
  - ○ The vTPM: This is achieved via encrypting and hashing the transferred data.
  - ○ The LMDF: This is achieved by using encryption and hashing algorithms.
  - ○ The Role-Based Migration: This is not achieved since no encryption of hashing is provided.
- **Requirement 4:** Protection against attacks, intrusions and malicious codes.
  - ○ The CoM Framework: This is not achieved since there is no applied mechanisms to ensure the integrity of the VMs or the host devices.
  - ○ The vTPM: This is achieved using the TPM standard.
  - ○ The LMDF: This is not achieved.
  - ○ The Role-Based Migration: This is partially achieved through the Secure Hypervisor module.
- **Requirement 5:** The presence of mechanisms to detect and report suspicious activities.
  - ○ The CoM Framework: This achieved through implementing IDs and IPs systems as part of the NSE-H environment.
  - ○ The vTPM: This is not achieved due to the absence of detection and prevention systems.
  - ○ The LMDF: This is not achieved.
  - ○ The Role-Based Migration: No detection mechanisms are implemented in this approach.

TABLE II. A COMPARISON OF THE DISCUSSED APPROACHES

Security Dimensions	The CoM Framework	The vTPM	The LMDF	The Role-Based Migration
Access Control	Yes	No	No	Yes
Authentication	Yes	Yes	No	Yes
Non-Repudiation	Yes	Yes	No	No
Data Confidentiality	No	Yes	Yes	No
Communication Security	No	Yes	Yes	No
Data Integrity	No	Yes	Yes	Yes
Availability	Yes	No	No	Yes
Privacy	Yes	Yes	Yes	No

- **Requirement 6:** Protection against vulnerabilities in the migration software.
  - The CoM Framework: This is not achieved as there is no applied mechanisms to ensure the integrity of the migration protocol,
  - The vTPM: While mechanisms are used to ensure the integrity of the VMs, no mechanisms are deployed to ensure the integrity of the migration software.
  - The LMDF: This is not achieved.
  - The Role-Based Migration: This is not achieved.

Furthermore, table II analyses each discussed solution in the context of X.805.

V. CONCLUSION

There is a clear shift towards delegating computation to the Cloud and virtual systems. To benefit from the full potential of these systems, features like live migration seems to be crucial for both system performability and availability. However, security of live migration is still in its infant stage. Therefore, the paper investigates the security issue of live migration using the X.805 standard. Eight security threats have been analysed and discussed in that context. The paper also discusses a number of proposals to secure live migration. The discussion highlights the fact that different proposals have addressed different security threats; however, no integrated approach has been proposed to address all of them. Therefore, our future work is to develop a comprehensive security framework that addresses the highlighted security threats in this paper. All in all, we believe that live migration is a useful tool for performance optimization and incident response tasks. However, live migration itself creates new security problems that need to be addressed before any wide-scale implementation.

REFERENCES

[1] Vmware, Inc. *Virtualization Overview*, White Paper. http://www.vmware.com/pdf/virtualization.pdf. [Last Accessed 04-12-13].

[2] F. Travostinoa, P. Daspitb, L. Gommansc, C. Joga, C. de Laatc, J. Mambrettid, I. Mongaa, B. van Oudenaardec, S. Raghunatha, Ph. Yonghui Wange, *Seamless live migration of virtual machines over the MAN/WAN*, Future Generation Computer Systems 22. 901907. 2006.

[3] Ch. Clark Keir , C. Clark , K. Fraser , H. Steven , J. Gorm Hansen , E. Jul , C. Limpach , I. Pratt , A. Warfield, *Live Migration of Virtual Machines*. In Proceedings of the 2nd ACM/USENIX Symposium on Networked Systems Design and Implementation. 2005.

[4] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, *A view of cloud computing.* ,Communications of the ACM, 53(4):5058, April 2010.

[5] J. Shetty, M R. Anala, G. Shobha. *A Survey on Techniques of Secure Live Migration of Virtual Machine*. International Journal of Computer Applications (0975 8887), Volume 39 No.12, February 2012.

[6] H. Ballani. *A study of prefix hijacking and interception in the internet*, In Proceedings of ACM SIGCOMM, 2007.

[7] Z. Saman Taghavi, J. James, T. David. *A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks*. IEEE Communications Surveys Tutorials, Volume:15, Issue:4, 2013.

[8] C. Cowan, F. Wagle, Calton Pu, S. Beattie, J. Walpole. *Buffer overflows: attacks and defenses for the vulnerability of the decade*. Information Survivability Conference and Exposition. 2000.

[9] Z. Zeltsan. *ITU-T RecommendationX.805 and its application to NGN*. http://www.itu.int/ITU-T/worksem/ngn/200505/presentations/s5-zelstan.pdf. [Last Accessed 04-12-13].

[10] De. Martin, *Asynchronous Transfer Mode. Solutions for Broadband ISDN*. Prentice Hall. 1993.

[11] M. Aiash, G. Mapp, A. Lasebae, R. Phan. *Providing Security in 4G Systems: Unveiling the Challenges*. Sixth Advanced International Conference on Telecommunications. 2010.

[12] M R. Anala, J. Shetty, G. Shobha. *A Framework for Secure Live Migration of Virtual Machines*. International Conference on Advances in Computing, Communications and Informatics. 2013.

[13] D. Perez-Botero. *A Brief Tutorial on Live Virtual Machine Migration From a Security Perspective*.

[14] S. Biedermann, M. Zittel and S. Katzenbeisser. *Improving Security of Virtual Machines during Live Migrations*. Eleventh Annual Conference on Privacy, Security and Trust (PST). 2013.

[15] J. Oberheide, E. Cooke, F. Jahanian.*Empirical Exploitation of live migration of virtual machines*. Proc of Black Hat DC, March 24, 2008.

[16] A. Back, U. Mller, and A. Stiglic. *Traffic Analysis Attacks and Trade-Offs in Anonymity Providing Systems*. Information Hiding, volume 2137 of Lecture Notes in Computer Science, page 245-257. Springer, 2001.

[17] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage.*Hey, You, get off my cloud: exploring information leakage in third-party compute clouds*. In Proceedings of 16th ACM conference on computer and communication security, 2009, pp 199-212

[18] Cisco, Inc, *Cisco IOS Software Configuration Guide, Release 12.2SX (VLAN Configuration Guidelines and Restrictions)*. http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/ 12.2SX/configuration/guide/vlans.pdf. [Last Accessed 04-12-13].

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

[20] C. Xianqin, G. Xiaopeng, W. Han, W. Sumei, L. Xiang. *Application-Transparent Live Migration for virtual machine on network security enhanced hypervisor* . Research paper. China Communications. Page 32 42, 2011.

[21] Trusted Computing Group. http://www.trustedcomputinggroup.org /resources/tpm_main_specification

[22] S. Berger, R. Caceres, K. A. Goldman, R. Perez, R. Sailer, and L. Doorn, *Virtualizing the trusted platform module*. in In USENIX Security, pp. 305320, 2006.

[23] Xen Project. http://www.xenproject.org/.[Last Accessed 05-12-13].

[24] T. Dierks, E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.2*. Request for Comments: 5246 . 2008.

[25] W. Wang, X. Wu, B. Lin, K. Miao, X. Dang, Secured VM Live Migration in Personal Cloud. In Proceedings of ICCET, China, 2010.

[26] P. Dewan, D. Durham, H. Khosravi, M. Long, and G. Nagabhushan. *hypervisor-based system for protecting software runtime memory and persistent storage*. In Proceedings of the 2008 Spring Simulation Multi-conference (Ottawa, Canada, April 14 - 17, 2008).