A Trusted VM-vTPM Live Migration Protocol in Clouds

Hong Zhou[1,2], Juan Wang[1,2], HuanGuo Zhang[1,2]
1. School of Computer, Wuhan University, Wuhan, China
2. Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, Wuhan Wuhan, China
for_zh@whu.edu.cn, jwang@whu.edu.cn, liss@whu.edu.cn

***Abstract*—Security has been regarded as one of the greatest problems in the development of Cloud Computing. The trusted computing provides the hardware-based protection for cloud computing security based on TPM. While vTPM using in cloud environment still faces technical challenges, among which VM-vTPM live migration has been unsolved yet. In this paper, the trusted VM-vTPM live migration scene in clouds and its security and performance requirements are analyzed. Furthermore, a trusted VM-vTPM live migration protocol and its detailed design are presented. At last, the protocol was evaluated from the aspects of security and performance. As far as we know, the trusted VM-vTPM live migration protocol based on the pre-copy is firstly proposed in this paper.**

Keywords- Cloud Computing security; virtual Trusted Platform Module; live migration; protocol

I. INTRODUCTION

Security issue has become the largest challenge in cloud computing field with its rapid development. Trusted computing technology can provide effective solutions for this problem by integrating itself into cloud computing environment and providing cloud services in a trusted way. Currently, the research on trusted computing in cloud computing has been a hot topic of cloud computing security.

The trusted computing provides physical hardware support for cloud computing security based on TPM chip [1]. When TPM is used in cloud, its virtualization is essential. Berger's TPM virtualization method [2] can map a physical TPM into multiple virtual trusted platform module (vTPM) to present corresponding vTPM instance for each VM. vTPM offers the user the same functions such as binding, seal and key storage as physical TPM for better security protection of cloud computing system, while vTPM using in cloud environment still faces technical challenges, among which live migration of VM and its corresponding vTPM (VM-vTPM) has been unsolved yet.

VM migration in cloud computing has two scenarios: static migration and live migration. The live migration can move a running VM from a source node to a destination and resume the VM at the destination node. Some important services are supported by live migration, such as on-line maintenance, on-line upgrade and load balance. However, the current VM live migration lacks sufficient security mechanism to protect VM from being attacked during igration and lacks effective methods to migrate corresponding vTPM.

Aiming at the problem, we design a trusted VM-vTPM live migration protocol by the method of Pre-Copy. On the foundation of trusted computing, this protocol enhances the security protection of VM and its corresponding vTPM sensitive information in migration process. Futhermore, the optimization of live migration performance especially downtime ensured that cloud providers could constantly serve users during VM-vTPM migration.

The rest of this paper is organized as follows. Section 2 introduces relative studies. Section 3 provides trusted VM-vTPM live migration requirement analysis and design points. Section 4 presents a trusted VM-vTPM live migration protocol. Section 5 is the evaluation on the protocol. Section 6 concludes the whole article.

II. RELATED WORK

Berger proposed a software method to realize hardware TPM virtualization [2]. A physical TPM was mapped into multiple vTPMs to present corresponding vTPM instance for each VM. Attributed to the design ideas, the Xen system [3] supported the realization of vTPM. However, vTPM migration in Xen still has technical challenges to improve.

Other methods of TPM virtualization or vTPM migration protocols are found in the following research work [4]. Nevertheless, the problem of realizing the cooperation of vTPM and TPM in application system without interfering normal processing operations like live migration still needs further study. Besides, the current VM live migration lacks sufficient security mechanism. [5]

Aslam proposed a Trust_Token based VM migration protocol [6], which guaranteed that the user VM can only be migrated to a trustworthy cloud platform. In the protocol, only security was considered, but performance wasn't taken into account during VM migration.

PALM system [7] was proposed to ensure the confidentiality and integrity of protected data during and after VM live migration, while vTPM was not taken in this system.

Danev firstly proposed a secure VM-vTPM migration protocol [8], in which "suspend-transfer-resume" mode was used for migration operation instead of real live migration.

The VM-vTPM migration method was researched based on trusted environment in cloud computing [9], and

the way to VM-vTPM live migration was described, though correlative protocol was not presented.

On the basis of the research above, security and performance of VM-vTPM live migration were first comprehensively analyzed in this paper. Furthermore， a trusted VM-vTPM live migration protocol based on the pre-copy was firstly presented in the paper.

III. REQUIREMENTS ANALYSIS

A. Scene description

The cloud management server and other servers are involved in VM-vTPM migration process in clouds. Assuming the server required VM-vTPM migration is the source, and sends migration request to the cloud management server which decides the destination based on related resource strategy dynamically. The relative services would not be interrupted except for the suspension during migration process.

The research in this article is based on Xen system which is of excellent performance and open-source. All the involved servers are equipped with virtualization-supportive CPU, and physical TPM chips are set on the mainboard of servers. Also, each VM is provided with corresponding vTPM instance on the basis of TPM virtualization method in Xen system.

The trusted VM-vTPM live migration scene is shown in Figure 1.

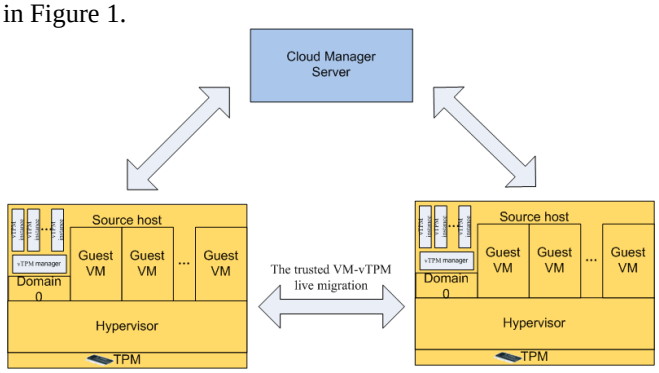

Figure 1. The trusted VM-vTPM live migration scene

B. Requirements Analysis

1) *A security requirements*

The security requirements provided by Danev [8] are of great importance for the protocol related to VM-vTPM migration.

a) *VM-vTPM Confidentiality and Integrity:* The confidentiality means that distrusted entities cannot obtain any meaningful VM-vTPM information, and the integrity ensures that any illegal modification should be detected and handled before and after VM-vTPM migration process.

b) *Initiation Authenticity:* Only exactly identified trusted entities can send VM-vTPM migration process request; distrusted ones are not allowed to do this.

c) *Preserving the Trust Chain:* Only trusted entities can receive right VM.

2) *Performance requirements*

The migration performance index refers to downtime and migration time. The target of VM-vTPM live migration is to possibly shorten the downtime and migration time to increase service usability.

a) *Migration time:* the period from sending migration command to resuming VM-vTPM at the destination.

b) *Downtime:* the time when VM-vTPM doesn't respond external service request. The downtime influences service usability more than the migration time, thus it should be preferentially optimized.

C. Design points

Based on the study of practical Xen system migration mechanism, the design points are analyzed as follows:

1) *VM migration*

The VM live migration contents mainly consist of memory pages and CPU state. Due to the large sizes, the external storage files are shared to the net through NFS but not the migration to shorten the downtime to the least.

The current VM live migration protocol is provided with little security mechanism, which should be added to protect data confidentiality and integrity.

2) *vTPM instance migration*

The vTPM in Xen system is implemented in software. The internal state data of vTPM instance including SRK, EK and PCRs etc. are stored on disk. So their integrity and confidentiality must be protected during the migration of vTPM instance.

Danev's vTPM model showed that the VM-vTPM exist in the same running environment—Dom U domain of Xen, while practically they are in different environment in Xen system, that is, VM exists in Dom U and vTPM instance in Dom 0 of Xen.

Technical challenges are still in the way of migration of vTPM instance in Xen system.

3) *VM-vTPM synchronous migration*

VM-vTPM state synchronization is of great importance in VM-vTPM migration.

To achieve this synchronization, Danev adopted the "suspend-transfer-resume" mode, whereas it cannot meet the requirements of live migration.

On the foundation of Xen system migration mechanism, the migration timing shall be mainly considered for VM-vTPM state synchronization. Here migration of vTPM instance is designed in stop-and-copy period.

IV. PROTOCOL DESCRIPTION

A. Protocol outline

Based on the research above, this article presents a trusted VM-vTPM live migration protocol which contains three phase: authentication, remote attestation and secure data transfer. The protocol is shown in Figure 2.

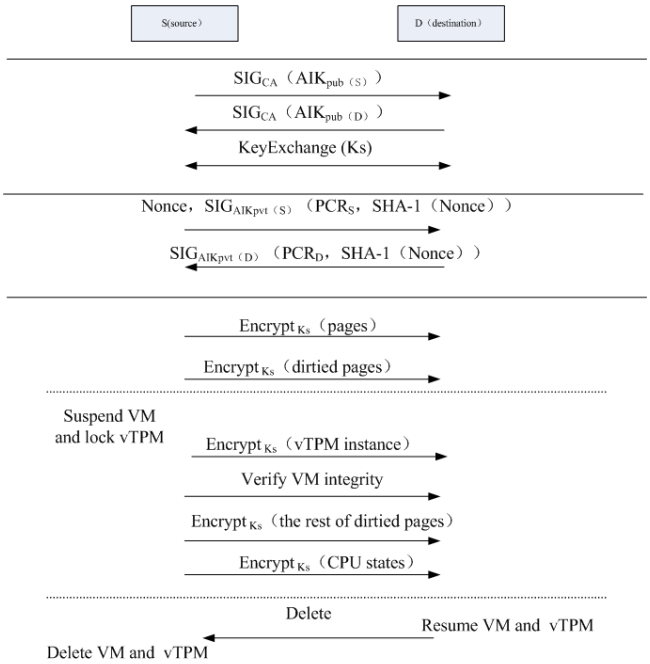

Figure 2. The trusted VM-vTPM live migration protocol

1) Authentication

The source S and destination D mutually authenticate using AIK public key certificate and exchange session key (K_S) to establish the secure channel for later communication. This process could be actualized by SSL protocol [10], and the session key (K_S) is to encrypt transmission data.

2) Remote attestation

The source S and destination D respectively attest platform integrity. The process for remote attestation of source S is: firstly, the source S implements the following procedures: a. produce a timestamp Nonce; b. SHA-1(Nonce); c. call TPM_quote command with Nonce hash value and obtain TPM platform integrity certificate signed by AIK private key, among which PCR value is defined as SHA-1 hash value including VMM measurement value; d. the source S sends the results of Nonce and quote to the destination. Secondly, the destination D implements the following procedures: a. obtain Nonce hash value from S platform integrity certificate and confirm that it is produced in this conversation; b. get PCR value from S platform integrity certificate and compare it with the known reference of VMM measurement value to assure the integrity. Up to this process, remote attestation of the source S by destination D is finished.

Similarly, the destination D platform integrity can be validated.

3) Secure Data transfer

After the mutual authentication and remote attestation of the source and destination, the authenticity and integrity are mutually proved and secure migration between source and destination, i.e. secure data transfer could be carried.

B. Detailed design

VM-vTPM migration is practically conducted in secure data transfer. The detailed design is presented as follows.

The pre-copy method [11] is used in trusted VM-vTPM live migration to shorten downtime. With the command, the migration is cut into three stages: pre-copy stage, stop-and-copy stage and resume stage.

Meanwhile, trusted VM-vTPM live migration protocol strengthens the security of live migration in Xen system, to protect VM-vTPM confidentiality and integrity in migration process.

1) Pre-Copy

VM-vTPM runs on source during this stage. All the memory pages are transferred from the source to the destination, and then the pages changed before (dirty pages) are transferred by rounds. When dirty pages are little enough or the frequencies reach to a certain number, the pre-copy is finished.

The memory pages from source are encrypted by session key (K_S) during transferring.

2) Stop-and-copy

At the first of this stage, the source suspends VM and locks corresponding vTPM.

The next tasks are: a. migrating of vTPM instance; b. verifying the integrity of vTPM instance; c. copying the last dirty pages; d. copying CPU state.

In comparison with VM live migration mechanism in Xen system, vTPM instance migration and integrity verification are new tasks.

The flow chart of stop-and-copy stage in VM-vTPM live migration is shown as Figure 3.

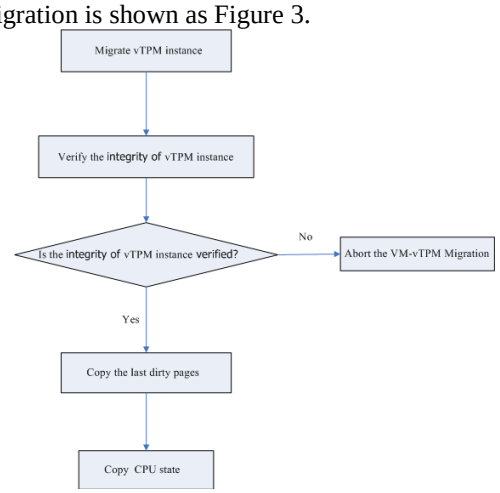

Figure 3. The flow chart of stop-and-copy stage

During this process, vTPM instance, memory pages and CPU state are encrypted with session key (K_S) and the integrity of vTPM instance is verified.

Considering the live migration performance requirements, the integrity verification of memory pages and CPU state are skipped to shorten VM-vTPM downtime.

3) Resume

VM-vTPM resumes on destination in the resume stage. Then the original VM-vTPM is deleted and the resource is recycled on source.

V. PROTOCOL EVALUATION

A. Security analysis

In the protocol, the source and destination identify mutually and exchange session key (K_S) to establish the secure channel for later communication. The VM-vTPM data are encrypted with K_S and the integrity of vTPM instance is verified. The mechanism based on secure channel satisfies the basic requirements of VM-vTPM confidentiality and integrity protection.

The accomplishment of source identity authentication and later integrity verification show the destination has ensured source authenticity and integrity. Since the migration starts from the source, the source confirmation has met the basic requirements of initiation authenticity.

In the remote attestation, source and destination mutually verify platform integrity so that only trusted entities can receive right VM. That has met the basic requirements of preserving the Trust Chain during the whole migration.

In conclusion, this protocol has satisfied the basic security requirements of VM-vTPM live migration.

B. Performance analysis

The increased security protection leads to the live migration performance loss. At the same time of satisfying the security requirements, this protocol majorly optimizes the downtime and reduces performance loss to the largest possible. The pre-copy method used in trusted VM-VTPM live migration protocol remarkably shortens VM-vTPM downtime to realize the VM-vTPM live migration.

Considering the live migration performance requirements, integrity verification of memory pages and CPU state are skipped in the stop-and-copy stage. In the protocol, the performance cost of downtime mainly causes by vTPM instance migration and vTPM integrity verification to shorten VM-vTPM downtime during migration.

The adopted secure channel technology based on SSL protocol realizes the encryption transmission of memory pages, CPU state and vTPM instance data, which reduces the loss of downtime and migration time as well as satisfies VM-vTPM confidentiality protection.

Thus, this protocol has met the VM-vTPM live migration performance requirements as much as possible.

VI. CONCLUSION

This paper firstly studies the trusted VM-vTPM live migration scene in cloud environment and analyze the trusted VM-vTPM live migration requirements of security and performance. Furthermore, with the research of the live migration mechanism in Xen system, the design points of trusted VM-vTPM live migration were presented. Based on all that above, a trusted VM-vTPM live migration protocol and its detailed design are described. At last, the protocol is evaluated from the aspects of security and performance. By satisfying the basic security requirements of VM-vTPM live migration, the protocol meets VM-vTPM live migration performance requirements to the largest possible.

In the paper, security and performance of VM-vTPM live migration are first comprehensively analyzed , and a trusted VM-vTPM live migration protocol based on the pre-copy is firstly proposed. On the basis of implementation mechanism design in Xen system, this protocol tried to solve the problem of trusted VM-vTPM live migration in real Cloud environment.

ACKNOWLEDGMENT

This work is sponsored by National Natural Science Foundation of China (91018008, 61003268) and the Huawei Technologies Co., Ltd. collaborative research project.

REFERENCES

[1] Trusted computing group: trusted platform module (TPM) specifica-ions, https://www.trustedcomputinggroup.org/specs/TPM, 2006

[2] Berger S,Caceres R, Goldman KA, et al., “vTPM : Virtualization the Trusted Platform Module”, Proceedings of the 15th Conference on USENIX Security Symposium (USENIX-SS’06), Aug 2006, Berkeley, CA, USA. pp.305-320.

[3] B ARHAM P,DRAGOVIC B, FRASER K, et al., “XEN and the art of virtualizaiton”, Proceedings of the 19th ACM Symposium on Operating Systems Principles (SOSP 2003)[C]. Bolton Landing, NY USA,2003. pp.164-177.

[4] Stumpf F, Eckert C, “Enhancing trusted platform modules with hardware-based virtualization techniques”, Proceedings of the 2008 Second International Conference on Emerging Security Information, Systems and Technologies (SECURWARE’08), Aug 2008,Cap Esterel, France. USA: IEEE Conference Publications, pp.1-9.

[5] Leelipushpam, P.G.J., Sharmila, J., "Live VM migration techniques in cloud environment — A survey," Information & Communication Technologies (ICT), 2013 IEEE Conference on, pp.408-413, April 2013

[6] Aslam, M., Gehrmann, C., Bjorkman, M., "Security and Trust Preserving VM Migrations in Public Clouds," Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, pp.869-876, June 2012

[7] Fengzhe Zhang, Yijian Huang, Huihong Wang, Haibo Chen, “PALM: Security Preserving VM Live Migration for Systems with VMM-Enforced Protection”, Proceedings of 3rd Asia-Pacific Trusted Infrastructure Technologies Conference (APTC-2008), pp.9-18, 2008.

[8] Danev B,Masti RJ, Karame GO, et al., “Enabling Secure VM-vTPM Migration in private clouds”, Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC'll), Dec 2011,Orlando, Florida, USA. USA: ACM Press, New York, NY, pp.187-196.

[9] Ling Li，Research on Some Issues of Data Security in Cloud Computing Services， PhD thesis, University of Science and Technology of China, 2012 (in Chinese)

[10] The transport layer security (TLS) protocol v 1.1 txt.pdf. http://www.rfc-editor.org/rfc/pdfrfc/rfc4346.

[11] C. Clark, K. Fraser, Steven H, J. G. Hansen, E Jul, C. Limpach, I. Pratt,and A Wareld. “Live migration of virtual machines”, Proceedings of the 2nd ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI), May 2005, Boston, Massachusetts, USA, pp. 273-286.