An approach to ensure the trustworthiness of cloud platform using the trusted chain

Guan Wang
Dept of Computer and Science
Beijing University of Technology
Beijing, China
wangguan@bjut.edu.cn

Lubaihui Gao
Dept of Computer and Science
Beijing University of Technology
Beijing, China
gaolugrace@sina.com

Abstract—IaaS (Infrastructure as a Service) provides users with "pay" calculation mode in cloud platform. Users can obtain computing or storage resources he needed from suppliers to load related applications and just rent that part of the resources to pay for at the same time. However, users start to lose their control over data access under this condition so that security issues bear the brunt. In this paper, we take advantage of the idea that trusted computing combine with current existing technology in IaaS. By embedding TPM chip into the cloud platform, we can use remote attention with proof of the trust chain information to prove whether remote nodes are trustworthiness or not. Thus, it can guarantee the security of the aspect of hardware in IaaS.

Keywords- cloud computing; IaaS; trusted computing; the trusted chain

I. INTRODUCTION

In recent years, cloud computing has became the preferred way for more and more cloud providers and cloud users apply to work, since it realizes many characteristics, such as sharing among platforms, virtualization, multi-tenant and on-demand pay. However, because of losing control of data and systems, the integrity and confidentiality of data are facing serious security threats.

The idea about combining cloud computing platform with the trusted computing is a good way to solve cloud security and in fact there have been many programs based upon this solution. Tal Garfinkel et al proposed Terra(1) model, utilizing a trusted virtual machine monitor TVMM to divided multiple virtual machines sharing hardware platforms, thereby preventing the owners of the host from examination and intervention calculated to ensure that the virtual security machine. But TVMM only provides protection for the operation of the VM. Santos(2) proposed a trusted computing platform TCCP which makes use of TCG specification to establish .However, the issues including generation and management about a trusted node, the migration of virtual machine and other issues, are still at the theoretical stage. It needs to be further confirmed by means of a prototype system.

Above mentioned studies, the paper proposes the introduction of a trusted third party (TC) of remote nodes to ensure the credibility of nodes in cloud environment (a third party is always trusted by default): Firstly, we design a node construction with a TPM chip combining the technology existing IaaS layer currently. Then we build the trusted chain above this platform and TC verifies the integrity of the chain of trust in order to determine whether the node is credible. After that, TC records nodes validated into itself trusted list. Moreover, there is a problem which cannot be ignored that the TC's trusted list is in danger of being attacked and tampered, therefore this paper also proposes a node registration agreement to ensure the safety of TC's list of trusted nodes, thus enhance user's confidence in the cloud.

II. A CLOUD NODE PLATFORM EMBEDDED WITH TPM CHIP

This platform is based on Xen hypervisor (3) and TPM virtualization technology to build the platform. VMM use several different types of virtual machines to set up several different execution environments and isolate from each other; at the same time it also provides an abstraction on the TPM hardware through a virtual TPM interface. vTPM is mainly used in the trusted virtual machine. The virtual machine handles trusted privacy-sensitive data and its operating system only run the minimum number of processes. This can effectively reduce the number of security vulnerabilities. Before starting, the security of trusted virtual machine is measured by a hardware hash engine for measuring a proprietary process to complete the measurement. Then the measured values are mapped to the PCR in the vTPM instance so that they have access to the virtual machine. In addition, VM0 is responsible for the starting, stopping and configure of virtual machine. It is a privileged virtual machines and access to the hardware TPM directly.

A. *Trusted Virutual Machine*

Trusted Virtual Machine (TVM) is used to run sensitive software program and trusted third party verify sensitive virtual components of pre-installed programs. Whenever a virtual machine is created, a corresponding virtual machine instance is initialized. PCR0-PCR15 hash value is used to store the TPM hardware. The PCR values in the vTPM instances are stored from PCR16. Meanwhile, in order to further reduce defects, any changes of client system in the virtual machine are not to be written back to the disk image.

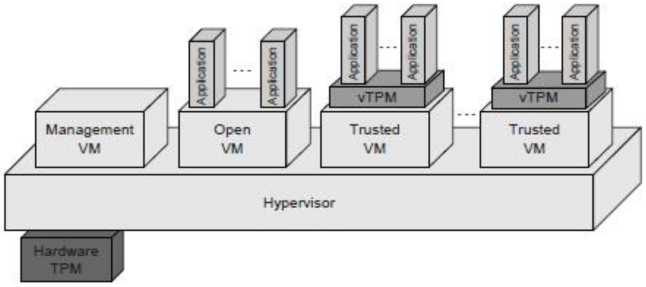

Figure 1 Node architecture

B. *vTPM*

IBM proposed vTPM (4) structure that provides a single virtual vTPM in a software manner for each virtual machine, thus avoiding the resource conflicts of multiple virtual machines sharing physical TPM. TPM features such as secure storage and cryptographic functions not only can be skillful applied to the virtual machine, but also the integrity of the software can be proved by the remote attestation with vTPM. It's worth nothing that a VM instance needs to bind with a corresponding vTPM. To ensure this binding relationship has been maintained, there is a list of relationships between VM and vTPM instance. vTPM managers are responsible for generating and managing vTPM instance.

III. ESTABLISH THE TRUSTED CHAIN

With the help of establishing the trusted chain in a terminal platform (5) and remote attestation, the paper demonstrates the credibility of the node. According to the mentioned platform architecture, we use this model as a basis to build the trust chain transfer model. Establishing progress is divided into two stages: the first stage is from CRTM to OS kernel stages. The hash values of various parts are secure stored in the physical TPM. Second stage is from vTPM Manager in Domain0 to applications. Trust metrics within the second stage of the virtual machine are measured by vTPM instances and results are stored in the PCR of the vTPM. So as introduced above, the measured values of physical and virtual platform are stored in two different PCR. The following table is a mapping in PCRs between the vTPM and TPM:

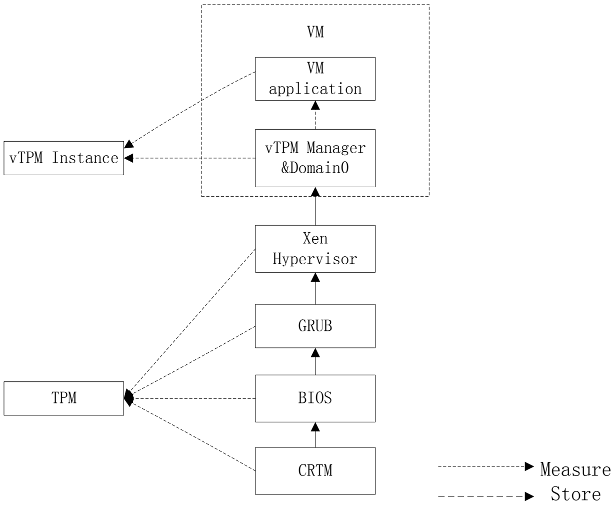

Figure 2 The model of the trusted chain in cloud server platfrom

PCR(platform configuration registers) are defined in the TCG.It represents changes about the platform configuration. These PCRs are initialized before starting for the integrity of the measured value storage system components. What's more, a software component is measured by CRTM before performing; Then the corresponding hash value will be combined with the current value stored in PCRs, namely: TPM_Extend(PCR_N,VALUE)= SHA-1(PCR_N||VALUE). SHA-1 is the hashing algorithm provided by the TPM; || represents join. The progress of trusted transmission is that starts from the trusted toot and then determine the credibility of the next level of the node.

A. *The Trusted Chain on The Physical Platform*

The first stage is the trusted chain establishment from CRTM to OS kernel when the platform starts up .The integrity of all components are stored in the physical TPM provided. After power, TPM chip initializes the trust chain firstly and PCR0-PCR8 reset to 20 bytes zeros. When finishing beginning with the CRTM, it calculates own code using SHA-1 and extends to the hash value of PCR0. Then BIOS gains control of the system to measure BIOS and GRUB. There are three stages that GRUB is loaded to the operating system kernel: stage1, stage1.5 and stage2.Stage1 is in charge of calculating the SHA-1 hash value of stage 1.5 code which will be extended to PCR4 and come into Bootloader stage. Stage1.5 measures and loads current configuration file .SHA-1 hash value of stage2 code is calculated and extended to PCR4.After that it's loaded into memory and executed. Finally stage2 provides interactive interface and is loaded into OS kernel according to default configuration. Before reading the boot directory andloading the kernel image file, it calculates thecorresponding SHA-1 hash value to make sure the trustworthy about the kernel configuration file. Since the trust chain establishes in the kernel image, thus ensure the credibility of platform launch.

B. *The Trusted Chain on VM*

The second stage is the trusted chain establishment from VMM to OS when a virtual machine is running. Within this stage, measurement is completed by vTPM instance and corresponding results are stored in the vPCR. Remote attestation realizes the integrity verification mechanism for the virtual machine. There is a solution called static load-time measurement in VM .Terra is an example of such early. It realized measurement belonging to VM. The progress starts when each VM image has loaded into the desktop. As for Xen, region 0 creates a trusted root. The integrity of VM is collected through the chain so that they can be extended to the PCR or ordered vPCR.

As introduced above, the measured values of physical and virtual platform are stored in two different PCR. The following table is a mapping process between the vTPM and TPM PCR:

TABLE I. TWO TYPES OF PCR

PCR	TPM	vTPM
0…7	Integrity measurements of CRTM、BIOS、Boot loader	Integrity measurements of CRTM、BIOS、Boot loader
8…15	Integrity measurements of Xen hypervisor and os core	Integrity measurements of Xen hypervisor and os core
16…	none	Integrity measurements of the application on VM

IV. VERIFICATION OF THE TRUSTED CHAIN

Verification process is completed by remote attestation, which referred to a trusted third party to take part in. There is a list of trusted third party trust designed to store information trusted nodes. Verification process is divided into three steps: credible third party challenge to the node, establish the trusted chain and check the authenticated identity, check the integrity of the trusted chain.

- Credible third party challenge to the node. Nonce can identify with each session to ensure the uniqueness of the session.
- Establish a chain of trust list information and check the authenticated identity. The authenticator is calculated by the hash value of the TPM_Extend operations to complete the integrity of the measurement system components and the measurement results are stored in a series of PCR to ensure its integrity in order to complete the update. In this series, different sequence or any type of hash values will have different results. AIK private key is then used to prove the identity of its own platform encryption, namely TPM_Quote operation sends the encrypted result back to the third party. AIK certificate authenticator is provided to verify the authenticity of a third-party inspection by side to verify that the certificate is to verify the identity of the party.
- Check the integrity of the information chain of trust list. Authenticator takes advantages of the log according to node measures in this process in order to simulate TPM_Extend operations and calculates value of the expected PCR. PCR is then compared with the actual values what are supplied to the authenticator. AIK verifier only needs to use the public key to decrypt to get the real unforgeable PCR. If the result is the same as the description of the chain of trust, it proves that this node platform is credible. Then add this information to the trusted node list of trusted third party.

V. CONCLUSION

In the cloud computing environment, the user start to loss d cloud computing platform to further enhance the user's trust in the cloud.

REFERENCES

[1] GARFINKEL T,PFAFF B,CHOW J, et al. Terra: a virtual machine based platform for trusted computing[C]//Proceedings of the 19th ACM Symposium on Operating Systems Principles (SOSP'03).New York, NY,USA:ACM Press,2003:193–206.

[2]. N. Santos, K. P. Gummandi, and R. Rodrigues, "Towards Trusted Cloud Computing", in Workshop on Hot Topics in Cloud Computing, San Diego, CA,2009.

[3].Barham P, Dragovic B, Fraser K, et al. Xen and the Art of Virtualization. In:Proceedings of the 19th Symposium on Operating Systems Principles. Bolton Landing, NY, USA, 2003, 164-177.

[4] .S. Berger, R. Cáceres, K. A. Goldman, et al., "vTPM: Virtualizing the Trusted Platform Module," in 15th USENIX Security Symposium, Vancouver, B.C., 2006.

[5].Trusted Computing Group. Trusted Platform Module Main Specification, Part 1:Design principles, Part 2: TPM structures, Part 3: Commands.Version1.2.