ATLANTIS PRESS
Advances in Computer Science Research, volume 70
2nd International Conference on Mechatronics Engineering and Information Technology (ICMEIT 2017)

Research and Design of Virtual Machine Based on User Trusted Security Strategy

Qichao Yang [a], Rongyu He [b,*] and Lichen Shi [c]
Information Engineering University, Zhengzhou 450000, China
[a]yangqichaoo@foxmail.com, [b]994058517@qq.com, [c]fanzihua@163.com

Keywords: Trusted cloud platform, the trust-source integration, User configurable, integrity measurement.

Abstract. Cloud users want to get a full control of the virtual computing resources in a cloud platform, a trusted cloud computing technology provides a reliable measure in the root for the cloud platform, but it couldn't provide fine-grained credible support services, and can't meet the demand of users the flexibility of security policies, aiming at the problem, we introduce LCTVM model to construct a virtual TPM for user, to achieve the user's security configuration by building TPM_Admin component effective load of the strategy, We design the VTRAP agreement to ensure that the user and session key between TPM Admin in negotiation, and verify its attacks in the state of effective security. This article formulated the strategy table user program security levels to meet user personalized security requirements, through the establishment of trust based on the platform and the user's dual source virtual trusted root, effective integration platform for trust and user trust. Validation and analysis show that this design of user-oriented trusted virtual machine can provide not only meet the demand of multi-user credible measures guarantee, and can realize the user customized security policies customized.

1. Introduction

Cloud platform virtual machine instance to users in IaaS (infrastructure) environment, The user does not need to purchase a computing device, but using computing capacity existed in a large cloud, such not only saves the cost of users, at the same time, make the whole network architecture greatly improved on capacity utilization. the safety of the virtual machine is the operation such as the user's data protection, data storage, data add and change the basis of security, How to ensure the cloud data integrity and confidentiality is a hotspot of research on the current cloud security, On the one hand, The reason is users don’t have physical control of the cloud data, on the other hand the centralized resource management makes the cloud environment relative to the user in a closed state, the user does not have the cloud service provider's right to know of the operation[1]. At the same time users do not have control over and under the condition of right to know, users can't confirm for the security of the data on the cloud, unable to establish an effective trust. This uncertainty based on safety concerns is the bottleneck of the development of cloud computing technology, so the research how to establish an effective trust between the user and the cloud service provider has very important theoretical and practical value.

2. Background

A trusted cloud computing can be summarized research thought is the basis of the virtual machine for the user to establish physical source of trust, This role shall be borne by the TPM hardware equipment, TPM equipment is a standard security chip with multiple security protection function. From the perspective of the infrastructure of the cloud hosting platform only a centralized TPM, cannot adapt to cloud multi-tenant provide trusted computing service mode for multiple virtual machine, a one-to-many relationship can lead to the collapse of the whole platform[2]. Hardware virtualization technology for the effective use of TPM in a multi-tenant environment provides a new train of thought,

Copyright © 2017, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

through virtualization technology to construct multiple virtual TPM, called v TPM, enables each virtual machine has to provide one-on-one service guardian v TPM provide trusted computing service.

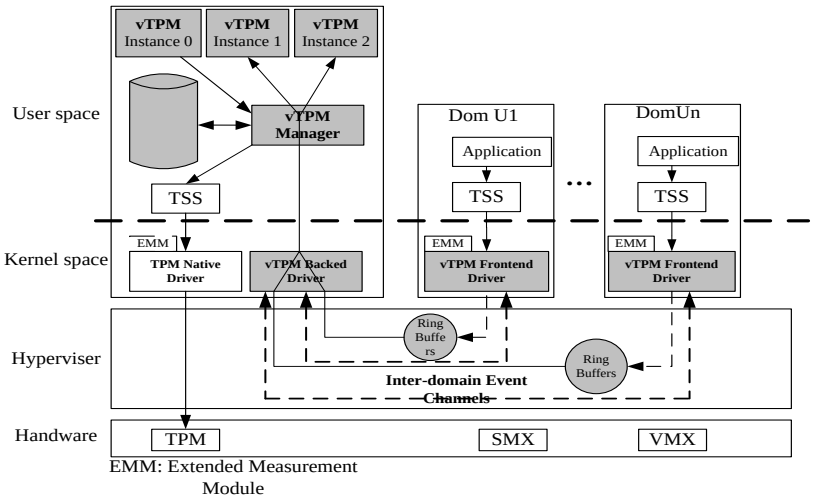

Fig 2.1 vTPM architecture diagram

Literature[2] propose a model based on PGP trust and RAA - CCP protocol proposed a simple, safe, extensible virtual v TPM, but due to the trust model based on the platform only trust the source, the lack of security configuration based on the user; Literature [3] proposed a improved based on the strategy of DAA and Privacy CA TCCP model, improved the security and reliability, but it directly on the basis of security v TPM architecture, lack of specific build process; Literature [5] proposes a trusted cloud platform based on the alliance of TPM management model, can achieve a few user configuration credible passed to the virtual machine, it was based on the destruction of the original cloud platform at the cost of physical architecture, a lack of practicality[3]. Overall existing scheme has the following general defects:

(1)physical TPM limited resources caused by structural defects, no dynamic expansion of storage resources (such as PCR register), cannot be limited user segmentation between the measurements of storage, once some user information leakage, could threaten other users' data security, even destroy the security of a cloud platform;

(2)Unable to effective utilization of resources of physical TPM, may lead to multiple users the measurements of the virtual machine in the presence of PCR collision of the extended operation may (extended to register the same PCR) at the same time, leads to the virtual machine are organized, destroy the cloud of elastic dynamic demand;

(3)Unable to effectively collect user configuration to the security of virtual strategy, causes the user can only passive receiving cloud platform to provide security services, users lose control in the virtual machine safety, cannot build based on user trust trusted virtual machine, cannot satisfy the user's customized security services.

In this paper, aiming at the problems of the existing cloud Trusted platform, put forward the double trust source trust transfer model stepped trust Chain model, virtual machine (Ladder - like Chain of Trusted for the VM, LCTVM), a credible virtual machine design based on user trust, meet the security needs of the user personalization promotes the credible degree of the virtual machine.

3. LCTVM Model Design

3.1 LCTVM Model

In figure 2.1, on the basis of LCTVM model to improve the TPM trust chain model and complement, between physical TPM and the trust of the virtual machine chain adds a TPMAdmin components. The privilege of the component is located in the high safety level domain, physical TPM and the isolation mechanism to ensure the integrity and security of the cloud platform. TPMAdmin is responsible for receiving a user security configuration information, and then use virtualization technology to create u TPM, The u TPM is responsible for guarding of the corresponding virtual

machine, u TPM is able to provide the same as the TPM hardware trusted computing services, such as a software component measurement and reporting, safety launch, virtual machine stepped trust chain model structure as shown in Figure 3.1.

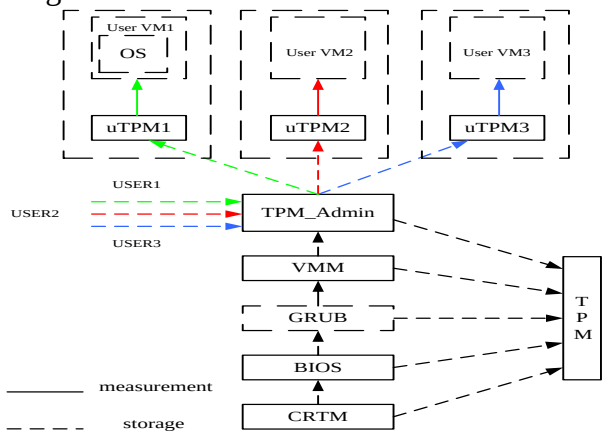

Fig 3.1 LCTVM model

LCTVM model constructed a kind of stepped security trust chain, the next level measure of integrity is the foundation of component measurement at the next higher level, through the slopes eventually establish the whole trust chain, trust of TPM measurement in order for the CRTM, BOIS, GRUB, VMM and TPMAdmin, measurement results are saved to the physics of TPM PCR register [4].

TPMAdmin function mainly includes two aspects, first, make by means of software simulation software TPM physical as interface of the application of TPM and hardware, the same instruction set, which has the same function; Second, load the user security strategy, according to the user's security requirements on different in a virtual machine with users in the corresponding uTPM loading different metrics, provide each user with different configuration, reliable guarantee the diversity of user requirements.

3.2 TPM_Admin Structure

TPM_Admin includes two important components in the structure, the first is a software TPM, it is to build a virtual TPM execution component, through software simulation, in the form of building a virtual TPM provides users with trusted computing services such as integrity measurement, data signature; Second is virtual TPM manager (called UTPM manager) VTPM manager in the user's virtual machine and UTPM plays the role of a messaging, receive, parse, store, transfer, executing and retransmission request from user's virtual machine TPM, UTPM status information created, deleted, it is responsible for all the, migration, UTPM manager receives the user configuration needs call software TPM build a UTPM, TPM manager through "VM - UTPM" table maintains many virtual machine and UTPM corresponding relation.

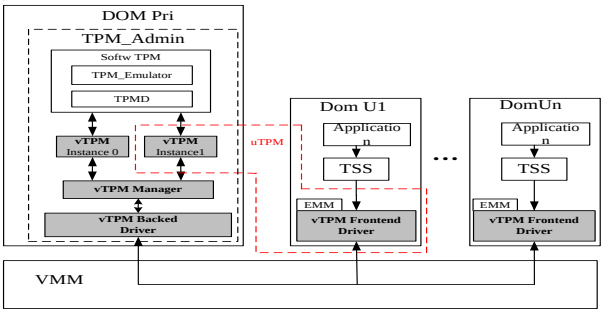

Fig 3.2 TPM_Admin structure

UTPM multi-instance run mainly by adding in the structure TPM_Admin daemon TPMD done, including in TPM_Admin divided into user space and kernel space, user space through the key driver module TDDL establish loose coupling relationship, with TPM_Admin TDDL's main function is to send TPM_Admin instruction, which involves the key function basically has: Tddl_GetCapability () and Tddl_SetCapability (), and are responsible for setting equipment attribute information.

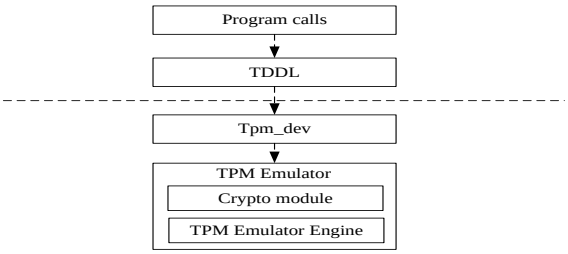

Fig 3.3 Soft - TPM operation process

Resident TPMD process memory space, through a Socket to listen from the user's request, split requests sent TPM_Admin, TPMD TPM_Admin startup mode by the load module to implement TPMD procedures, allows modules to load for many times, so as to create multiple virtual TPM instance.

3.3 The Realization of The uTPM

Each uTPM contains two parts, respectively is virtual vTPM Instance (virtual TPM Instance) and vTPM Frontend Driver (virtual TPM front drive), each uTPM support a user field full life cycle of trusted computing service, carrying up TSS (TCG Software Stack) operating system and user application. UTPM in the main by the VMM event channel and memory sharing mechanism to a virtual machine with users for information exchange, the main process is: the virtual machine send application Shared memory request to vTPM Frontend Driver, vTPM Frontend Driver receives a request for a virtual machine after application Shared memory, and TPM request is loaded into the Shared memory in the leaf, and Shared memory access authorization leaves to vTPM anyway: spreads over gse-backed loans Driver, vTPM Frontend Driver using interrupt notification time channel vTPM anyway: spreads over gse-backed loans Driver receives the TPM request information, vTPM anyway: spreads over gse-backed loans after the Driver receives forwarded to vTPM Manager request content, and the results back to the vTPM anyway: spreads over gse-backed loans Driver, then vTPM anyway: spreads over gse-backed loans Driver returned to the user according to the original path will result the virtual machine[5].

To combine to create a user profile information in accordance with different user uTPM examples, this paper design in TPM_Admin TPMCU (TPM Control Unit the Control Unit, it includes the need to create a uTPM all of the information, it is essentially a data structure, based on its load can realize creation, uTPM TPMCU for the whole system security level is very high, so it can be set to only allow TPM_Admin calls.

Fields of TPM Control Unit	
PCRs[0...8]	//Measurements of TCB
PCRs[9...23]	//Measurements of the virtual machine
Attestation Identity Key(AIK)	
Storage Root Key(SRK)	
Edorsement Key(EK)	
Edorsement credential(EK)	
M[i][j]	
...	

Fig 3.4 TPMCU structure

TPM_Admin in perform the user action request is the next, first of all, analyze allocation strategy, user will parse results according to TPMCU encapsulation structure, and then initializes the virtual TPM instance, complete uTPM configuration.

Multi-tenant patterns of cloud platform, decided to have multiple virtual machines at the same time [6]. In order to determine which user is launched a trusted virtual machine to the uTPM service request, for each uTPM in TPM backend driver provides a 4-byte identifier, established a "VM - uTPM maintained table" to maintain the user virtual machine with uTPM one-to-one relationship, uTPM execution as shown in figure 3.5.

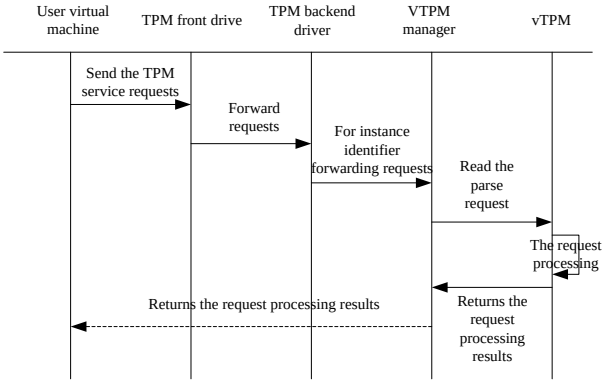

Fig 3.5 uTPM workflow

Specific steps process for:

Step 1: users virtual machine send TPM front drive TPM service request;

Step 2: TPM front drive after received from the user's request, do not handle directly forwarded to TPM backend driver;

Step 3: TPM backend driver after receives the request, by looking for a virtual machine with uTPM binding identifier, find the corresponding uTPM, add the information to request, to generate a new request sent to uTPM manager;

Step 4: after listening to the request, UTPM manager read requests for binding representation character parsed into the content of the request UTPM is sent to the corresponding operations carried out UTPM;

Step 5: uTPM perform the corresponding operation;

Step 6: uTPM will manipulate the execution result and identifier returned to uTPM manager encapsulation;

Step 7: UTPM manager read identifier to find the corresponding user virtual machine, through the back-end drivers and front drive virtual machines will be returned to the user request execution results.

4. User trust transfer

LCTVM model for the past exists only platform credit the source of the deficiency of single trust protection mechanism, joined the source based on the trust of the user security policy configuration, LCTVM model can add user security configuration strategy to TPM_Admin, generated by TPM_Admin components according to the security configuration of loaded for virtual TPM user security requirements, integration user double trusted sources and platforms [7].

4.1 The safety of the user strategy

This article designed the Remote proof protocol based on uTPM modules VTRAP (uTPM Remote Attestation protocol) to ensure that key agreement between users and TPM_Admin transmission. The definition function of the agreement are as follows:

F1: $TPM\_Unbind(msg,'K')$ Decryption function

TPM decrypt function, including parameters for decryption of the encrypted message.

F2: $TPM\_Extend(value,i)$ Extension function

TPM extension function, using the extension function integrity measurement can be extended to the corresponding number for PCR i register. The concrete implementation process with the following function $PCR_i^{new} = H(PCR_i^{old} \| value)$ and $PCR_{init} = 0$

F 3: $TPM\_Quote('AIK\_ID', nonce, i_1, ..., i_k)$

TPM measurement function provides the current TPM PCR value report, TPM measurement for the request operation returns with AIK encrypted value of PCR results.

VTRAP agreement includes user U, TPM_Admin TPM and hardware, the session key negotiation process as shown in figure 4.1, in which nodes represent TPM_Admin.

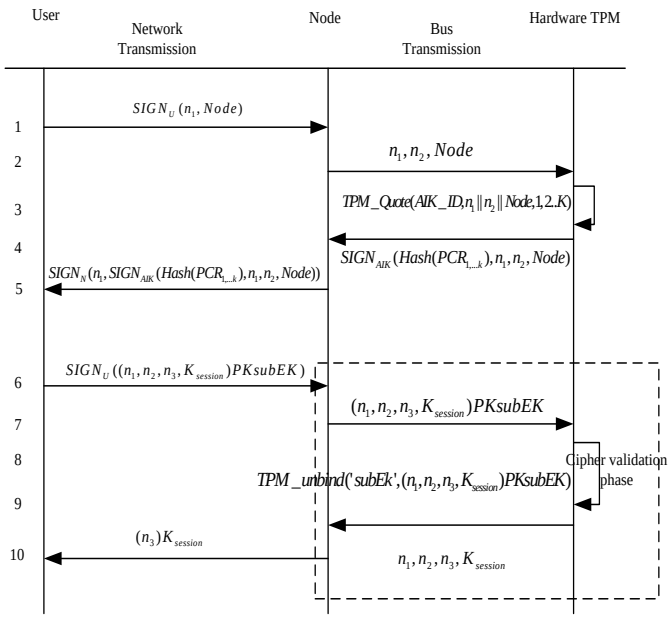

Figure 4.1 VTRAP process

Node hardware and TPM identity through the above steps to guarantee the safety of TPM_Admin and TPM hardware:

Step 1: the user signature random number and logo is sent to the node;

Step 2: to verify the identity of the user, will be forwarded from the user information to the TPM hardware, at the same time will generate random Numbers themselves along with;

Step 3: hardware TPM receives messages from the nodes, executive function $TPM\_Quote()$ With AIK key signature PCR value as the results sent to the current node.

Step 4: node with its own key signature since the TPM hardware and headed to the result of the user;

Step 5: after users receive the message, check the signature and the correctness of the random number, the user can U verify received PCR comparing with standard value, check nodes and the integrity of the TPM hardware.

The establishment of a user session key process:

Step 6: Users use the TPM encryption key $subEk$ for random number n_1, n_2 newly generated n_3 and session key $K_{session}$ as a message, and then sign the message is sent to the node N

Step 7: node N confirmation message, and then forwarded to hardware TPM;

Step 8: TPM use $TPM\_unbind()$ functions to decrypt the message;

Step 9: the decrypted results back to the node N;

Step 10: node N using the session key encryption random n_3 and return it to the user, then user authentication random n_3.

A. The safety of the user strategy load

User security strategy including user program security level table, the user configuration information, users to customize security services, users use the system image, etc., is one of the main user program security classification strategy table and system image, as shown in table 3.1:

Table 3.1 the user program security level strategy table

Level	Category	List items	content
Level 1	The operating system	Linux or windows	measurements
Level 2	drive	hardware driver	measurements
Level 3	Based on the software	TCG software stack, office software	measurements
Level 4	Configuration information	The user needs to install the software	Static or dynamic measurements

User virtual machine images load steps as follows:

Step 1: to measure the key software in the virtual machine, save the measurement;

Step 2: user use private key K_u to encrypt the virtual machine image VMI_u;

Step 3: send encrypted image to the image library, transmission security by security transfer protocol;

Step 4: users to send its own policy information to TPM_Admin;

Step 5: after TPM_Admin to receive information, analytical information security strategy, according to the requirements of policy configuration created uTPM;

Step 6: virtual machine monitor (VMM) recovery and use private key K_u to decrypt VMI_u;

Step 7: configuration for the user's trusted virtual machine by decryption step 6 VMI_u.

5. Experiment and analysis

VTRAP Protocol Security Analysis

Scyther automatic analysis tool is a kind of agreement, we use it to design in the third chapter verifies the safety and reliability of VTRAP, protocol verification results are as follows

```
$> time ./ scyther .py    --max-runs=20    --all-attacks
verification_scyther . spdl
Verification results :
claim id [tpmp,u1], Niagree : No attacks .
claim id [tpmp,u2], Secret ksession : No attacks .
claim id [tpmp,u3], Nisynch : No attacks .
claim id [tpmp,n3], Nisynch : No attacks .
claim id [tpmp,n1], Niagree : No attacks .
claim id [tpmp,n2], Secret ksession : No attacks .
real 0m6.029s
user 0m5.950s
```

Figure5.1 VTRAP validation

As you can see from the results of the validation:

(1) For a limited time VTRAP protocol can resist known replay and middle attack.

(2) Users and cloud platform and the success of the negotiation session key, and to ensure that key in addition to the two, does not have the third person.

B. LCTVM Advantage Analysis Model

Solution while introducing trusted computing users before the virtual machine environment, through physical TPM provide trusted computing service to the virtual machine, but there are obvious shortcomings.

Table 3.2 LCTVM advantage analysis model

Num	Application	H1	H2	H3	H4
1	libHX				●
2	ntpq	●			
3	PHP			●	
4	Firefox	●	●	●	
5	Lynx		●		●
6	Sudo1.6.4		●		●

Process of the experimental results show that in table 3.2 run-time trusted certificate model can effectively measure the actual application state of runtime, seven of the for the experimental dynamic attack are effectively according to the regulations set by the user H1, H2, H3, H4 untrusted state of measurement and reporting process.

6. Conclusion

Trusted cloud platform in virtual machine ensure that provide users with reliable, at the same time need the user security policy is loaded into the virtual machine. Aiming at the existing cloud platform to provide user oriented fine-grained credible support services, the introduction of LCTVM model, to construct a virtual TPM in the user. By building TPM_Admin component effective load of the strategy to achieve the user's security configuration, designed the VTRAP agreement to ensure that the user and session key between TPM_Admin in negotiation, and verify its attacks in the state of effective security, formulated the strategy table user program security levels to meet user personalized security requirements. Through the establishment of trust based on the platform and the user's dual source virtual trusted root, effective integration platform for trust and user trust. Main job next extend the virtual machine starts in the process of dynamic operation reliable safeguard mechanism, add more comprehensive virtual mobile attitude amount index, the research covers the kernel and user virtual machine application, comprehensive cloud platform dynamic credible measurement system.

References

[1] Phillips C, Swiler L. A graph-based system for network vulnerability analysis[C]//Proc of the 7th workshop on New Security Paradigms. New York:ACM, 1998:71-79

[2] Sheyner O. Scenario graphs and attack graphs [D]. Pittsburgh: Carnegie Mellon University, 2004

[3] Ammann P, Wijesekera D, Kaushik S. Scalable graph-based network vulnerability analysis[C], Proc of the 9th ACM Efff on Computer and Communications Security. New York:ACM, 2002:217-224

[4] M. A. Ajay Kumara, C. D. Jaidhar. Execution Time Measurement of Virtual Machine Volatile Artifacts Analyzers[C]// 2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS). IEEE Computer Society, 2015:314-319.

[5] Zhou Z J, Wu L F, Hong Z, et al. DTSTM: Dynamic Tree Style Trust Measurement Model for Cloud Computing [J]. Ksii Transactions on Internet & Information Systems, 2014, 8(1):305-325.

[6] C. L. Forgy. Rete:a fast algorithm for the many pattern /many object pattern match problem[J]. Artificial Intelligence, 1982, 19(1): 17～37