# Research and Design of Trusted Computing Platform

ZHOU Yun-ting[1, a], DENG Mao-lin[1], CHONG Yu-hai[1], JI Feng-zhu[1], HE Xiao-gang[1] and TANG Qi-jie[1]

[1]Xichang Satellite Launch Center, XiChang, SiChuan 615000, China

[a]zhouyt001@yahoo.com.cn

**Keywords:** Trusted Platform Module; Roots of Trust; Trusted Computing

**Abstract.** With the development of trusted computing, trusted computing model and trusted computing platforms are constantly changing, and becoming more and more perfect. In terms of the hardware platform, the trusted computing technology has been gradually matured. Many companies and businesses solve security problems by using trusted technologies. Trusted computing technology focuses on such as hardware, operating system and other aspects, wishing to build a complete, credible and reliable trusted platform. In this paper, the structure of the trusted platform has been described. Focus on Protected Capabilities, Integrity Measurement and Attestation which are the representative characteristics, some analysis and researches have been proposed. And analyze the main parts and priorities of the designing process of trusted platforms.

## Introduction

The early 70s of last century, Anderson J P first proposed the concept of a trusted system (Trusted System), known as dependable computing[1]. The organization of the Trusted Computing Platform Alliance TCPA (Trusted Computing Platform Alliance) was led by several major international IT giants, the Compaq, HP, IBM, Intel and Microsoft in October 1999. And its members are all over the world, on all continents of the main manufacturers. TCPA defines the Trusted Platform Module with safe storage and encryption (TPM). in March 2003, TCPA reorganized as TCG (Trusted Computing Group), and released TPM master specification (v1.2) in the same year[2-4]. Its purpose is widely to use the Trusted Computing Platform under the hardware-based security module in computing and communications systems in order to improve overall security.

Because of the openness of the design of personal computer, software security solutions inherent defects and other reasons, the vulnerability of computing platform has attracted the attention of scholars, the security of computing platforms' is becoming increasingly important. Trusted Computing is to solve the existing open, distributed computing security environment from these two aspects. computing platforms which Exist now are open platforms. Although they are flexible but the hardware cannot establish trust security with the third-party. Some agencies developed a corresponding closed platform, though high security is not being widely used. Trusted Computing proposed a trusted platform based on both aspects.

## Architecture of Trusted Platform

Trusted Platform does not change the architecture of the platform, and also has the verifiability the features of both closed and open platforms, it requires only a very low cost chip - Trusted Platform Module [5]. Trusted Computing Platform has two main features. (1) Operations on the Trusted Computing Platform must be authorized and authenticated, any authorized user cannot use the platform to work. (2)Trusted Computing Platform will check the consistency of the system, system starts from a trusted source, it will verify BIOS, operating system in turn, and the application then, which will form a chain of trust to ensure that the system platform has not been altered or attacked. There are usually three roots of trust in a trusted platform: root of trust for measurement, root of trust for storage and root of trust for reporting.

 

To have a credible platform, fundamental functions such as Protected Capabilities, Integrity Measurement, Attestation, Data isolation and protection and Storage and reporting should be included. Now trusted platform already includes applications and infrastructure of networks, which forms a complete architecture as shown in Figure 1.

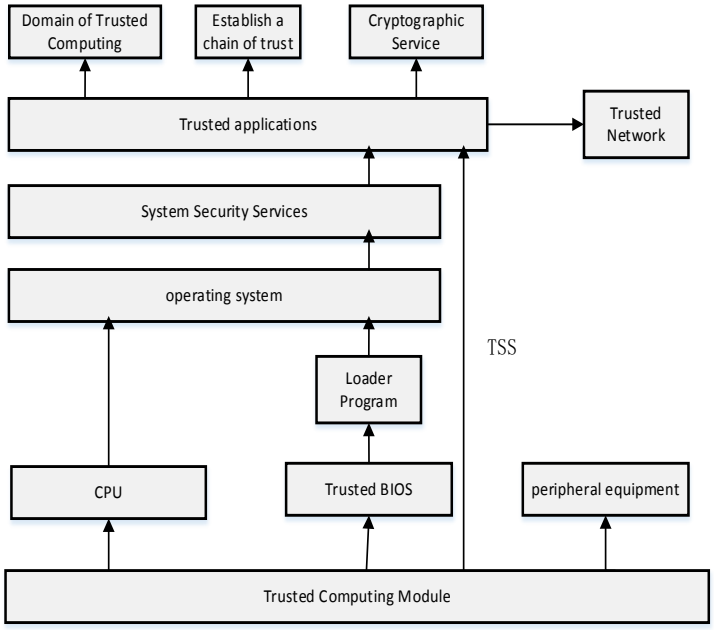


Fig.1 Architecture of Trusted Platform

The whole system can be divided into three layers: TPM, TSS and application software. The goal of designing TSS is to use TPM-enabled applications provide a unique entry, provide access, management, and resource release, etc. It consists of two parts, TCG (TSS core service) and TSP (TSS service provider). TSS platform software from the structure can be divided into three layers, from bottom to top respectively is TDDL, TCS and TSP, which are all running in user mode.

TCG believes that if the departure begins from an initial trusted root, during the each conversion of the platform computing environment, this trust can be maintained (trust chain (Chain of Trust))and not be destroyed by the way of transfer. The platform computing environment is always credible. The core of trusted computing is the Trusted Platform Module, which is the original root of trust. In general, after the platform is established, we believe that TPM and BIOS is absolutely credible.

## Trusted Platform Module

The core of trusted computing technology is the security chip based on the TPM. TPM is a hardware chip, which is the trusted root of trusted platform to provide protection for computer equipment from the underlying hardware, attached to an existing PC, servers and other environments, and provides a variety of security-related functions. [6-7]The main part containing cryptographic computation and storage components and other parts.

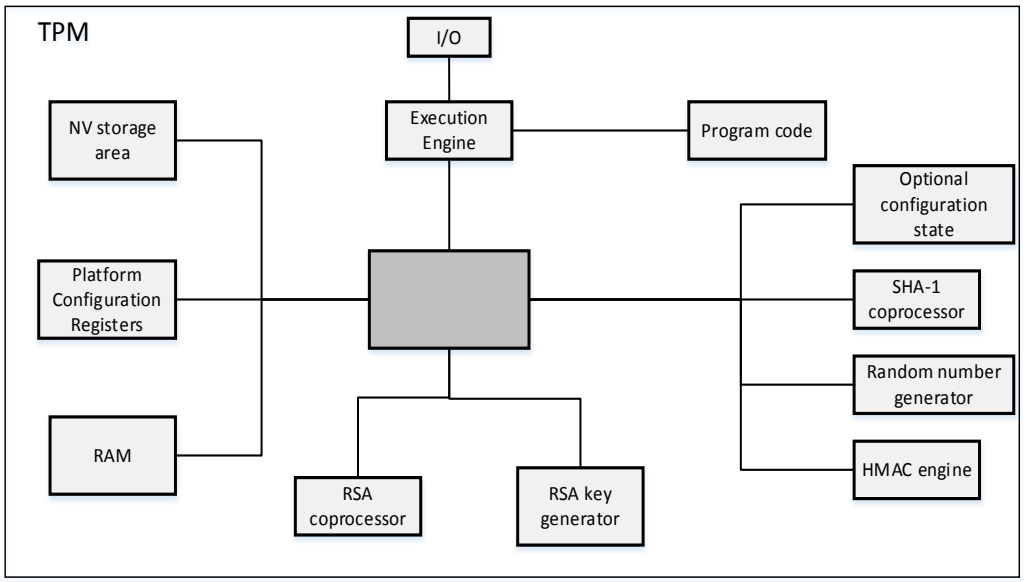


Fig.2 Structure of the Trusted Platform Module Chip

TPM mainly includes a microprocessor, Flash, random number generator, RSA engine, the HMAC engines, as shown in Figure.2. Asymmetric encryption and signature authentication are implemented by RSA coprocessor and keys. Integrity measurement is accomplished by the SHA-1 coprocessor, any symmetric can used for encryption algorithm. HMAC engine is used to verify the correctness of the entered command. Execution engines determine and implement the appropriate procedures based on the input command from I/O port. NV storage area save TPM internal state data, etc. Platform Configuration Registers (PCR) is to save the platform integrity metric.

So in the function, TPM can be divided into the cipher algorithm section, part of platform configurations, and to protect secret key data storage section, and command protocol verification section.

TPM interacts with the external programs is implemented by way of command. For each external program command format sent to the TPM has a special document definition. Each command is divided into two parts, request command and return command. TPM is mainly using single-process model, only one command can be sent to TPM at the same time, The next command will continue to be sent to the TPM. When the TPM is in a state to execute the command, the commands entered could not be accepted, just as shown in Figure.3. Data is wrote to the memory-mapped IO space memory. After the data is written, The operating system sends an interrupt to notify the application by polling TPM state or TPM, then read the data returned from the specified IO address.

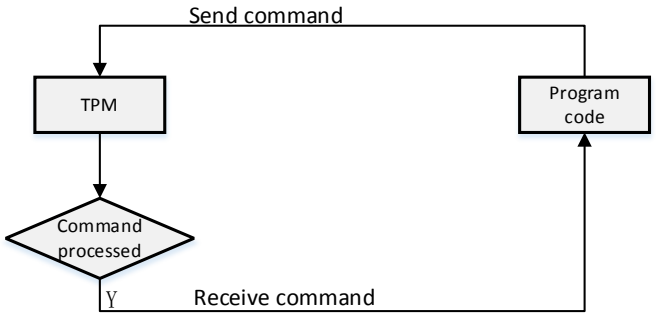


Figure.3 TPM command interaction methods

**Platform integrity measurement**

A feature of trusted platform is able to provide metrics and reports on the integrity of the platform. These functions are mainly achieved through the platform configuration registers (PCR), the endorsement key (EK) and the anonymous identity key (AIK), etc[8].

**Platform Configuration Registers (PCR).** In TPM, PCR is a critical component. it has

tamper-resistant features, Which is mainly used for storage the entity metric during the process of establishing a credible string.

A platform configuration register is usually a 160-bit memory cell. The number of PCR register is generally 16 or 24. All PCR were inside the TPM protected storage area. The measurement result of the platform integrity which is measured by SHA-1 algorithm is saved in PCR. The pass process of establishing a credible chain is to measure then pass, And metrics are in the presence of PCRs, Which will form a complete chain of trust trusted static.

For safety and the consideration of the number of PCR can be used, each metric is added to PCR as extended mode as follows.

$$[PCR(new)] = SHA-1([PCR(old) + (new - measured - value)]) \quad (1)$$

Connection between event data and the current value of CPR should be created first, then calculate the connector digest value, finally, store this value in the PCR. Thereby updating the value of PCR is not cumulative in nature. Different metrics for the same order for a PCR register, both updated values of the methods produce are not the same. That means, only a series of historical operation can be determined, the update results of PCR can be determined. Thus the PCR implicitly preservation of historical information of a platform. This feature of PCRs makes PCR can be used to store the state information platform during the entire operation.

Operating system, BIOS ROM, or other metric is stored in the PCR, these values are to be written from the start of the metric system startup. So no matter what state the platform (trusted or untrusted state), PCR can report real information of a platform. According to the update rule of PCR, Only restart a system, this information will be recorded. Accordingly, the measure in PCR represents the information of a platform.

**Integrity Report.** Although the information platform is saved in PCR, there is also a need for effective mechanisms can credible reporting platform information. This is the integrity report of a platform. TPM provides the endorsement key (EK) and proof of identity key (AIK) to report the platform integrity.

EK is a 2048 bits RSA key pair, public part of the key is called PUB EK, private part is PRIVEK. Each TPM contains a unique key pair. The key has been created before the end-user to receive the platform. The main function of EK is to generate AIK and establish the TPM owner.

AIK is a signature key, TPM use AIK to prove their identity. The entity which AIK signature, means it has been already passed by TPM treatment. Although the use of the AIK generate EK, but AIK does not contain any private information about the platform. Use AIK to sign its internal information data, it may include the PCR information, and other state of the TPM key information, which indicates that information is processed through the TPM. In reporting and measurement of TPM integrity, AIK plays a huge role, so generation process AIK and safety is very important. AIK generation process can be shown as Figure 4.

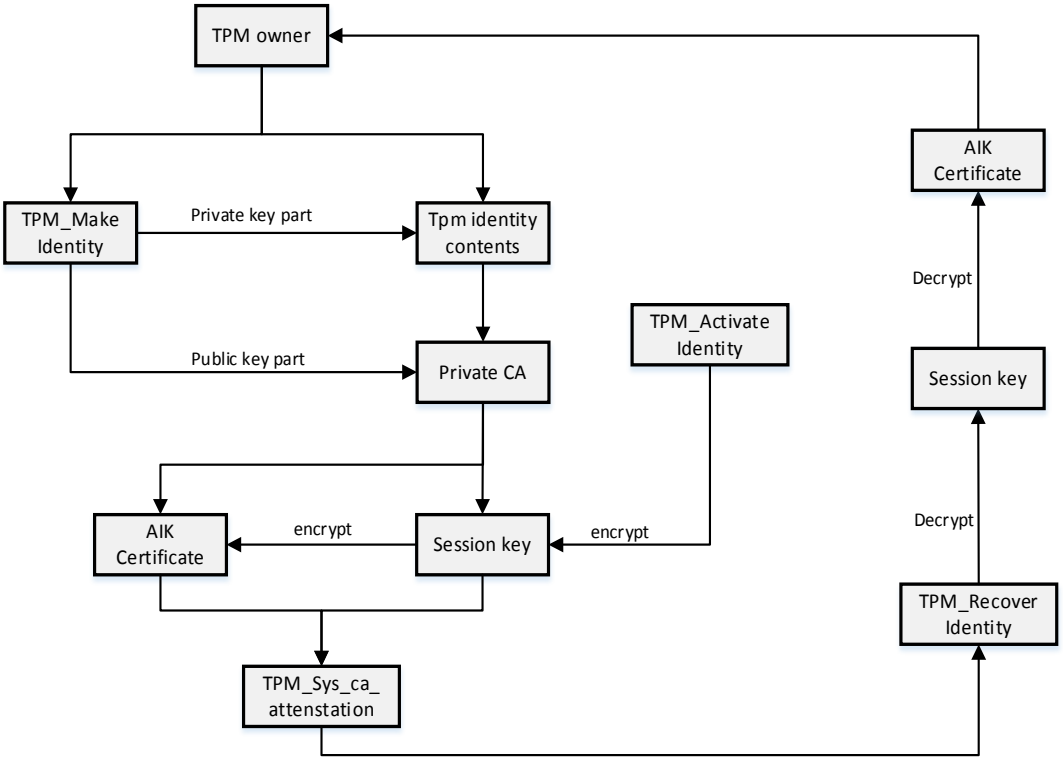


Fig.4 AIK generation process

**TPM commands interaction.** TPM and external entities (operating systems, processes, etc.) interact by way of command. TPM use sessions to complete message exchange mechanism , and the establishment of a session that means to establish a secure communications channel[9]. Session establishment process is also known as a verification process for TPM commands. A session is established through licensing agreements of TPM.

If one knows the owner password, through licensing agreements proving that he is the owner of the TPM, and can get ownership of the TPM. TPM owner and TPM control of each entity (for example: key) has authorization data (shared secret password), owner authorization data of the TPM is stored in the TPM, authorization data of the entities stored with other entities,so it can be loaded when use it. Purpose of TPM license agreement is the requester to prove that he knows the secret entity, so it is possible to use these resources (such as keys), evidence and knowledge sharing secrets.

TPM has three agreements for the requester to send the authorization data of knowledge of the evidence to the TPM: These are Object independent authorization protocol(OIAP), Object specific authorization protocol(OSAP) and Delegation specific authorization protocol (DSAP). OIAP offers multiple authorization session to any entity, OSAP provides authorization sessions to a single entity, And the new authorization information can be transmitted confidentially. DSAP support delegations from owner or entity.

TPM interacts with external programs by way of command. This command is transmitted in clear text, if it needs to transmit encrypted manner, a special session between the two entities should be established, this is the TPM transport session protocol. Purpose of establishing a transmission session is to encrypt the command in external programs in order to make it safety.

In the transmission session establishment, a shared secret can be created. By using the shared secret, this authorization can be achieved the session encryption command. When the transmission session establishment, the external programs use this session to execute the command to a package, that means to transmit the command for an encryption, and create a transmission session command, then sent to TPM. The establishment process of the transmission session can be shown as Fig.5.

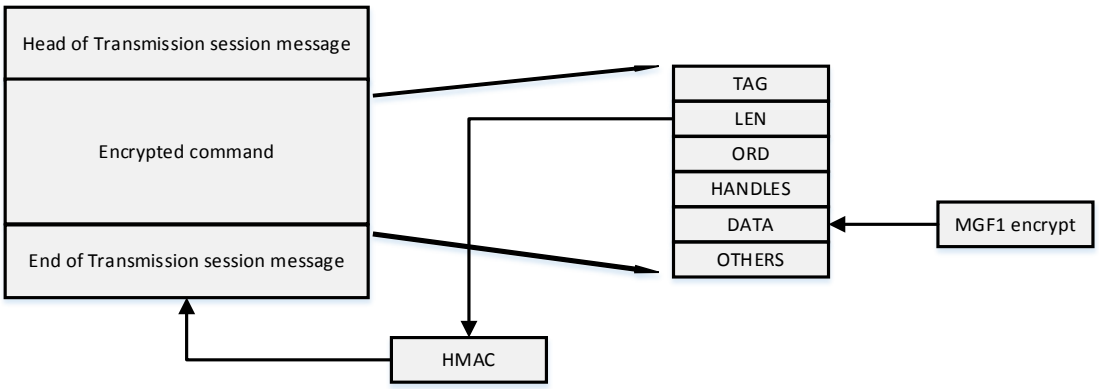


Fig.5 The establishment process of the transmission session

## Summary

In this paper, trusted platform module and trusted platform have been studied and discussed in depth. First, a detailed description of the internal composition in the Trusted Platform Module has been described. Then a detailed analysis has been discussed for several important functions of trusted platform. Such as integrity measurement, memory protection, and a variety of key management authorization and authentication protocols. Finally, the analysis of integrity measurement and TPM commands interaction has been carried out. And working principle of the trusted platform module, method of use have been proposed in depth.

## References

[1] L Vaquero. A break in the clouds: towards a cloud definition[J]. Computer Communication Review, 2008, 39(1):50-55

[2] S. Smith. Magic Boxes and Boots: Security in Hardware. IEEE Computer,2004, 37(10): 106 -109

[3] Peinado, M. Chen, Y. et al. NGSCB: A Trusted Open System. In Proceedings of 9th Australasian Conference on Information Security and Privacy. 2004. 13--15.

[4] Ahmad R Sadeghi, Christian Stüble.Towards multilaterally secure computing platforms – with open source and trusted computing, Information Security Technical Report.2005

[5] R. Macdonald, S.W. Smith, J. Marchesini, et al. Bear: An Open-Source Virtual Secure Coprocessor based on TCPA. Computer Science Technical Report TR2003-471, Dartmouth College, 2003

[6] Jan Camenish, Better Privacy for Trusted Computing Platforms, In European Symposium on Research in Computer Security 2004, 73-88

[7] R. Oppliger, R. Rytz. Does trusted computing remedy computer security problems? IEEE Security & Privacy, 2005, 3(2): 16-19.

[8] Fan He, Jing Len, Huanguo Zhang. Evolutionary testing of trusted computing supporting software based on genetic algorithms[C]. Proceedings of the 2008 International Symposium on Knowledge Acquisition and Modeling, Wuhan, China, 2008, 713-717

[9] T Garfinkel, B Pfaff, J Chow, et al. Terra: a virtual machine-based platform for trusted computing[C]. Proceedings of the 19th ACM Symposium on Operating Systems Principles, Bolton Landing, USA, 2003, 193-206