American Journal of Mobile Systems, Applications and Services
Vol. 4, No. 3, 2018, pp. 13-18
http://www.aiscience.org/journal/ajmsas
ISSN: 2471-7282 (Print); ISSN: 2471-7290 (Online)

Intelligent Terminal System Based on Trusted Platform Module

Dapeng Song*, Lei Peng

School of Medical Information Engineering, Taishan Medical University, Taian, China

Abstract

With the rapid development and popularization of mobile intelligent terminal devices, mobile intelligent terminals have become an indispensable part of people's study, work and life. The security issue about intelligent terminals is getting more and more attention. How to build a secure and trusted intelligent terminal environment is an urgent problem to be studied. Trusted computing technology is introduced in android-based mobile intelligent terminal. Trusted platform module is embedded into the intelligent terminal platform. Through the construction of the static credible chain, the hardware and the system are guaranteed to be secure and credible. Through the construction of the dynamic credible chain, the application installation and system operation process are guaranteed to be secure and credible. Through the transmission of the credible chain, it can ensure that the intelligent terminal system is safe and credible from booting to the whole running process. Thereby a secure and trusted intelligent terminal platform has been built. The experimental results show that the proposed method is reasonable and feasible. It can guarantee the operation of mobile intelligent terminal devices in a secure and trusted environment. It has certain promotion significance for promoting the development of terminal equipment in information security.

Keywords

Trusted Computing, Trusted Platform Module, Intelligent Terminal, Credible Chain

Received: September 18, 2018 / Accepted: October 9, 2018 / Published online: October 25, 2018

1. Introduction

With the rapid development and popularization, mobile intelligent terminals have become an indispensable part of people's study, work and life. The security of terminal devices is getting more and more attention [1-3]. With the development of the Internet, how to ensure the security and credibility of systems and applications of the terminal devices is also a concern. Therefore, it is urgent and important to carry out research on trusted computing of mobile intelligent terminal.

The trusted platform module (TPM) [4-5] is embedded into the intelligent terminal platform to construct a secure and trusted computing platform. Through the construction of the static credible chain, the hardware and the system are guaranteed to be secure. Through the construction of the dynamic credible chain, the application installation and operation are guaranteed to be credible. Under the guarantee of trusted measurement technology, the credible chain is transferred from the bottom to the operating system and then transferred to the application. The delivery of credible chain and the transfer of control right are controlled during the authentication process.

2. Trusted Computing Technology

2.1. Trusted Platform Module

According to the definition of trusted computing group (TCG)

* Corresponding author
E-mail address: dpsong@tsmc.edu.cn (Dapeng Song)

[4-7], the core technology of trusted computing is the trusted platform module. TPM is the key to the entire trusted computing platform, which uses TPM as the starting point for the trust root. Through a series of measurement, build a complete credible chain to achieve the credible goals of the entire platform.

TPM mainly performs three basic functions: public key authentication, integrity measurement, and proof [5, 8-9]. Through these three basic functions, the trust boot of the system and the trusted authentication of the terminal are realized. The public key authentication function means that TPM generates a key pair using a random number generator in the chip. Used for public key signature, verification, encryption and decryption, etc. Through the encapsulation of the private key and the encryption operation during data transmission, TPM can guarantee that the key will not be accessed by malware. The core key of TPM is the endorsement key (EK). For security and privacy reasons, EK is not directly used to encrypt or sign data. The main function of EK is to generate an attestation identity key (AIK) and establish the owner of the TPM. The storage root key (SRK) is generated by the owner of the TPM and is used to encrypt data. The key is invisible outside the chip, so even the key owner can't get the key, thus avoiding the attack. The integrity measurement function is the most central part of the entire trusted computing system. It prevents malicious code from obtaining a private key. During the trusted boot process, the hash value of the boot configuration information is stored in the platform configuration register (PCR). Once the platform is started, the data is sealed according to the value of the PCR. The proof function means that the TPM collects and submits a list of information for all measurement of PCR, and then signs it with the private key. So a trusted client can prove to the third party that its software is credible.

2.2. Trust Root

The core of trusted computing defined by TCG is to build a credible chain from the root to the BIOS, to the Bootcode, to the kernel, and to the operating system. It ensures that the entire system is trusted. Therefore, the trust root and trust measurement are two important components of the credible chain. In embedded systems, trusted booting of trusted devices is the key to the integrity of the entire system. Therefore, the construction of the trust root is very important. Because the trust root is the starting point of the credible chain, it is the basis for building trusted devices [10-12].

In intelligent terminal devices, the trust root is divided into root of trust for measurement (RTM), root of trust for storage (RTS), and root of trust for reporting (RTR). RTM is primarily used for integrity metrics. It is the calculation engine controlled by core root of trust for measurement (CRTM). CRTM is the first code executed after the trusted terminal is started. It is unchangeable and is the starting point of the credible chain. The CRTM initialization system starts and boots the TPM to work. The RTS is composed of the key an engine for storing encryption, which is used to store the hash value and digest value. It ensures that the delivery is credible. RTS needs to maintain the engine and integrity of the digest sequence. RTR is a calculation engine that reports the data held by RTS to the system. It must ensure the reliability of the data held. It is the basis and roots of the credible chain that ensuring all three roots are trusted [13].

2.3. Trust Measurement

The trust measurement in the credible chain is to obtain the credible eigenvalues. The construction of the static credible chain guarantees the trust from the low BIOS to the operating system. The construction of the dynamic credible chain is primarily a measure of the integrity for operating system and applications. The static measurement obtains the confidence eigenvalue of the metric object. These values are stored in the PCR. It is then compared to the coincidence value of the PCR to determine if the module is complete. The summary changes once the module is found to have changed. Therefore, the integrity of the module can be judged.

For trust measurement of the operating system and the underlying, the method of static metrics is mainly used. The message authentication method is implemented by using the HASH function, thereby reducing the amount of computation of the TPM. The trusted cipher module uses the secure HASH function SHA-1 as the calculation engine. The SHA-1 engine ensures that the system has certain prevent ability when it is attacked, thus achieving accurate metrics. Static metrics enable integrity metrics for each level of module. The integrity report can be passed to the next level through the previous level. This ensures that the system is a trusted, secure hardware and software environment.

In intelligent terminal systems, RTM is a trusted starting point. Measurements must be made before adding a component or before moving to the next component. The metrics for each component are stored in the PCR. The values on the PCR are stored in the order in which the components are started. At the same time, the metric log is also recorded in the startup sequence. Each time the system starts, the new value obtained by the metric does not directly cover the original value of the PCR, because the system cannot discriminate whether the new metric is obtained by the integrity metric or by the trespasser. Therefore, for security reasons, a cryptographic hash algorithm is needed to update the PCR.

2.4. Integrity Report

Integrity report is a report that the integrity metric provides to the outside world. While the trusted platform is measuring, it needs to provide the results and proof of these metrics to the outside world. The proof needs to be part of the handshake protocol to ensure the delivery of the credible chain. Therefore, reporting trust root and measuring trust root are two important parts of the integrity model and an important part of trust measurement. The delivery of trusted computing should follow a combination of integrity metrics and integrity reporting. To increase the metrics and delivery capabilities of trusted computing.

3. Construction of Trusted System Based on Android

The trusted computing platform based on intelligent terminals focuses on hardware and operating systems. It establishes a complete, credible and reliable trust platform. Basic functions such as data isolation and protection, identity authentication, trusted measurement, storage and reporting are implemented.

In the intelligent terminal of android operating system, the function library can be written in C language through the android native development kit (android NDK) [14-15] technology. That can solve the problem of low efficiency of Java. According to the security analysis, build a trusted computing platform architecture based on android. The android-based trusted computing platform architecture consists of three levels. From the bottom to the top, they are the hardware layer, the system software layer, and the application layer. The hardware layer includes the processor, the memory, the TPM chip, the peripheral device, etc. The system software layer mainly includes the calculation function library, the protocol algorithm library, the calculation library API, the trusted chip API, etc. The calculation function library uses the android NDK technology to write calculation functions that require in the application. The compute library API provides the packaged calculation functions to the user. The trusted chip API is a packaged trusted chip application interface. It includes related function libraries of trusted chips such as key generation, key management, and cryptographic algorithms. The protocol algorithm library calls the trusted chip API and the compute library API. It provides support for related protocols and algorithms for trusted computing applications. The application layer runs for a trusted computing application. The users can call various functions provided by TPM with trusted computing services. The trusted platform architecture based on android is shown in figure 1.

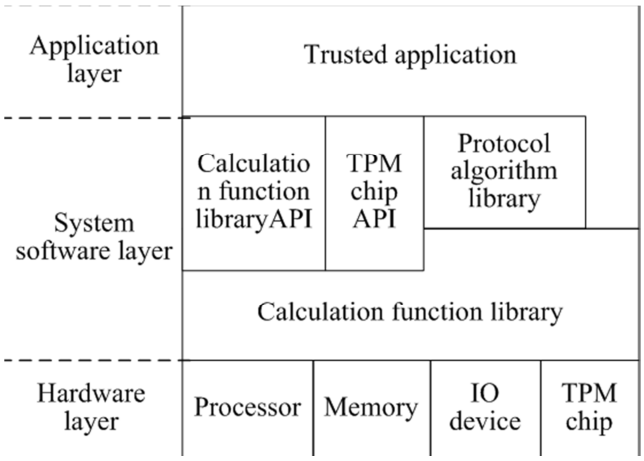

Figure 1. Trusted platform architecture based on android.

4. Construction of Credible Chain

4.1. Construction of Static Credible Chain

Through the construction of the static credible chain, the security of the hardware and the system can be guaranteed. The static credible chain refers to the credible chain from the trust root to the BIOS, Loader code, and operating system. Through the authentication and trust transfer, the trust is extended from the bottom to the entire intelligent terminal system, and finally the system is trusted. Through the trust measurement, the transfer of credible chain and control right are controlled during the authentication process. Each time control takes a step forward, the credible chain is passed forward step by step until it extends to the operating system. This creates a static credible chain from the CRTM to the operating system.

The integrity of the code needs to be measured before the transfer of control. The integrity metric is used to determine if the transfer is trustworthy. If it is trusted, go to the next module. The integrity metric is an eigenvalue for obtaining the credibility of the module for each stage. The module is judged to be complete by comparing the digest value of the eigenvalue with the contemporaneous value, thereby determining if the module is trusted. Once the module has changed, the summary will change. Through the changes of the summary, the integrity and credibility of the module can be judged. The eigenvalues of the metric are stored in the PCR. The credible chain is passed down through metrics, storage, and integrity reports to determine the credibility of the entire system.

4.2. Construction of Dynamic Credible Chain

Through the construction of the dynamic credible chain, it can ensure the security of the application installation and

system operation process. When an application in the system loads, it is first measured by the metrics module. The measurement results such as static element metrics and dynamic element metrics are obtained. Whether the application process belongs to a trusted process is determined based on predetermined metric rules and policies. If it is a trusted process, the control right is passed to the application process. After the application is loaded, the monitoring system will be started in order to prevent the modification behaviour of the malicious process. As long as the process modifies the system, it will be detected by the monitoring system immediately. Determine whether the modification behaviour is safe through integrity assessment and measurement. Only secure modification behaviour allows the application process to continue to run. The detection and integrity verification module has two main functions. One is to determine whether the behaviour of the process is permitted, and the other is to verify whether the integrity of the system is compromised. During the detection and integrity verification process, the monitoring system can quickly and timely isolate the operations that have occurred when the process is abnormal, ensuring that the system is not affected.

4.3. Trust Boot and Credible Chain Delivery

The source of the credible chain is CRTM. When the system platform is powered up, the first piece of code that is executed is CRTM. The data integrity metric is verified by a message authentication code (MAC). The MAC is implemented using a hash function. The calculation of the hash value is an operation that records the order of trust. The old value generated in the previous step is used together with the current new value as a parameter to calculate the metric value. The measurement and trust delivery process during the startup of the intelligent terminal platform is as follows.

(1) The CRTM in the trusted platform measures the BIOS code. The measurement results are saved in PCR and compared to the reference values stored in the non-volatile memory. If the metric is consistent with the baseline value, the BIOS is trusted and proceeds to the next step. Otherwise, the system terminates.

(2) The extension code of the BIOS is measured. The measurement results are saved in PCR and compared to the baseline values. The result is consistent with the baseline value, indicating that the system is credible and proceeds to the next step. Otherwise, the system terminates.

(3) The integrity metrics is performed on the bootloader. An integrity metrics report is generated and the metrics is stored in PCR. The resulting metric is compared to the baseline value. If certain metrics are met, it is credible. Give control to the bootloader. Otherwise, the system terminates.

(4) The bootloader measures the integrity of the operating system of the terminal. An integrity metrics report is generated. The metrics are stored in PCR and compared to the baseline values. If certain metrics are met, it is credible. Give control to the operating system. Otherwise, the system terminates.

(5) The operating system measures the integrity of file systems and applications. An integrity metrics report is generated. The metrics are stored in PCR and compared to the baseline values. If certain metrics are met, it is credible. Give control to the operating system application.

At this point, the startup process of the trusted platform and the delivery of the trust chain have been formed. In the process of trusted metrics, if the platform of the metric is found to be deviating from the security policy, the execution of the system should be suspended immediately to ensure the security of the system. If this metric deviation is within the allowed range, you can choose to make manual corrections or temporarily continue execution. The normal operation of the system is guaranteed by appropriate update components or security policies. The trusted boot mechanism requires that the verification policy be securely loaded onto the platform. After the platform is started, it is convenient to verify the platform in real time.

5. Experimental Results and Analysis

Due to the lack of hardware conditions, this experiment was verified by software simulation. The experimental environment uses Ubuntu 14.04, the Android operating system uses version 5.0.2, and the trusted environment is built using the TPM emulator 0.7.4 version. The TPM emulator can be used to simulate the function of the hardware TPM and has a rich driver library.

(1) Trusted platform launch

The experiment runs Android and TPM simulator. After the system starts, the running result is shown in Figure 2. It can be seen from the test results that the TPM starts the self-test successfully after the initialization is completed. Self-test content includes SHA-1 secure hash function, HMAC function, EK generation function, and RSA encryption and decryption function. After successfully completing the self-test, “wating for connections...” is displayed, indicating that the connection is waiting.

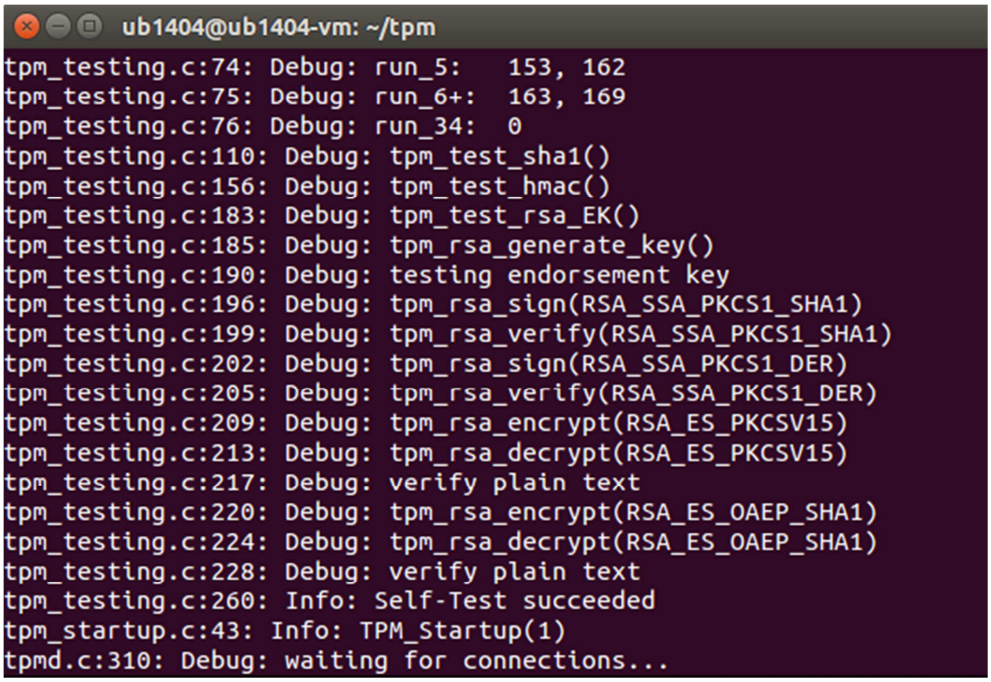

Figure 2. Trusted platform launch.

(2) Platform integrity metric

The PCR value is initialized. The saved measurement result file is loaded and expanded into the register PCR. The trusted metrics for the platform are complete. The PCR values of the platform system are shown in Figure 3.

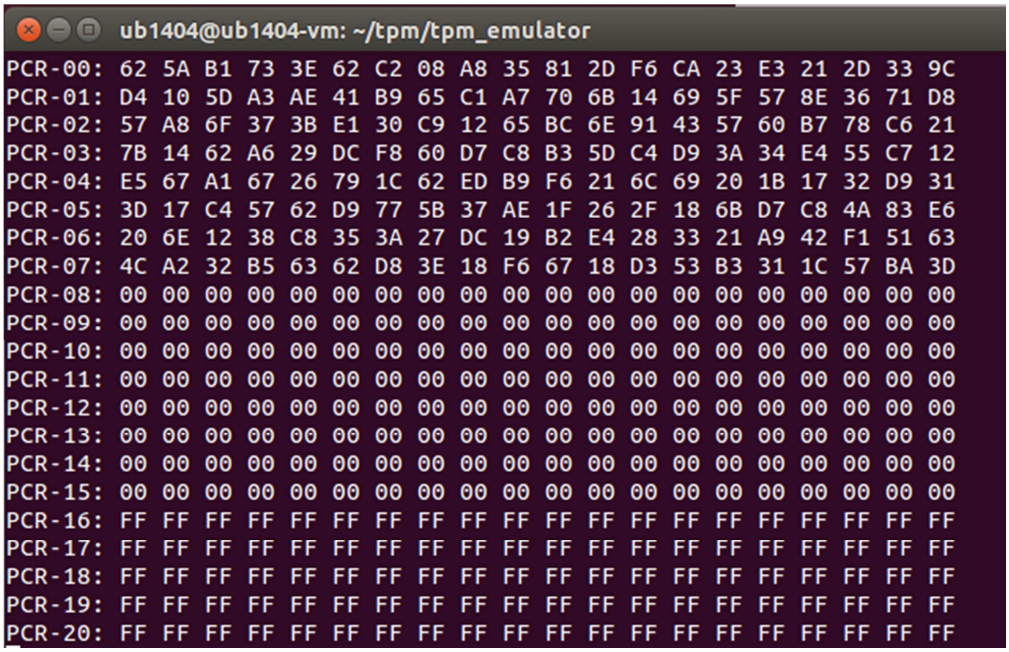

Figure 3. PCR value for platform integrity metrics.

(3) Platform integrity certification

The credibility of the platform is certified. The model is used to analyze the integrity metrics and a reference value is generated. This reference value describes the credible chain delivery. It is used as a reference for proof. It verifies the integrity of the platform by comparing the metric information of the typical platform and the reference value to the actual platform reference value. As shown in the figure 4 below, the platform integrity authentication is successful and the PCR value conforms to the trusted standard.

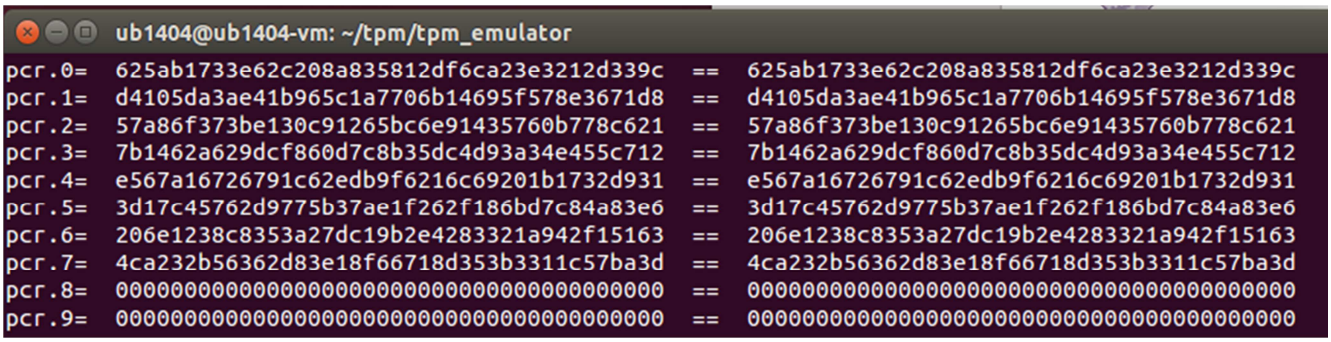

Figure 4. PCR value integrity certification.

The above experiments show that it is reasonable and feasible to embed the TPM module into the android operating system to achieve secure boot and integrity metrics. This method can ensure that the android system becomes a secure and trusted intelligent terminal system.

6. Conclusion

By introducing trusted computing technology into the android terminal device, the trusted startup of the terminal, the transmission of the trusted chain, and the measurement mechanism of the trusted computing are studied. The trusted platform module TPM is embedded into the trusted intelligent terminal platform to build a secure and trusted computing terminal platform. The research results have certain reference value for the security problem of intelligent mobile terminals.

Foundation Items

Shandong Provincial Science and Technology Development Program, China (No. 2014GGX101020)

Safe Production Major Accident Prevention Key Technology Program, China (No. shandong-0021-2015AQ)

References

[1] Si-Han Q. Research progress on android security[J]. J. Softw, 2016, 27: 45-71.

[2] Davidson D, Rastogi V, Christodorescu M, et al. Enhancing Android Security Through App Splitting[C]//International Conference on Security and Privacy in Communication Systems. Springer, Cham, 2017: 24-44.

[3] Zheng X, Yang L, Shi G, et al. Secure Mobile Payment Employing Trusted Computing on TrustZone Enabled Platforms[C]//Trustcom/BigDataSE/I SPA, 2016 IEEE. IEEE, 2016: 1944-1950.

[4] Trusted Computing Group. TCG Mobile Truested Module Specification. Specification，2016.

[5] Wang J, Shi Y, Peng G, et al. Survey on key technology development and application in trusted computing[J]. China Communications, 2016, 13(11): 70-90.

[6] Trusted Computing Group. Wikipedia [EB/OL]. [2017-05-01]. http://en.wikipedia.org/wiki/Trusted_Computing_Group.

[7] Kashif U A, Memon Z A, Siddiqui S, et al. Architectural Design of Trusted Platform for IaaS Cloud Computing[J]. International Journal of Cloud Applications and Computing (IJCAC), 2018, 8(2): 47-65.

[8] Asokan N, Ekberg J E, Kostiainen K, et al. Mobile trusted computing [J]. Proceedings of the IEEE, 2014, 102(8): 1189-1206.

[9] Xu M, Qin Z, Yan F, et al. Trusted Computing and Information Security [C] //Proceedings of the 11th Chinese Conference, CTCIS. 2017.

[10] Balasubramanian K, Abbas A M. Secure Bootstrapping Using the Trusted Platform Module[M]//Algorithmic Strategies for Solving Complex Problems in Cryptography. IGI Global, 2018: 167-185.

[11] Xu M, Qin Z, Yan F, et al. Trusted Computing and Information Security[C]//Proceedings of the 11th Chinese Conference, CTCIS. 2017.

[12] Maene P, Götzfried J, De Clercq R, et al. Hardware-based trusted computing architectures for isolation and attestation[J]. IEEE Transactions on Computers, 2018, 67(3): 361-374.

[13] Yu F, Zhang H, Zhao B, et al. A formal analysis of Trusted Platform Module 2.0 hash - based message authentication code authorization under digital rights management scenario[J]. Security and Communication Networks, 2016, 9(15): 2802-2815.

[14] Google. AndroidNDK [DB/OL]. [2018-09-01]. https://developer.android.google.cn/ndk/.

[15] Zhang H, Sun D, Xiao Y, et al. Construction of trusted computing platform based on android system[J]. American Journal of Mobile Systems, Applications and Services, 2015, 1(1): 54-58.