A Trusted Computing Architecture of Embedded System Based on Improved TPM

Xiaosheng Wang [1,1*], *Gaochao Xu* [2], *Yongfei Han* [1,2] *, and Yanchun Yang*[1,3]

[1] School of Information Technology, Shandong Women's University, Jinan 250300, P.R. China
[2] School of Computer Science and Technology School, Jilin University, Changchun 130022, P.R. China

Abstract. The Trusted Platform Module (TPM) currently used by PCs is not suitable for embedded systems, it is necessary to improve existing TPM. The paper proposes a trusted computing architecture with new TPM and the cryptographic system developed by China for the embedded system. The improved TPM consists of the Embedded System Trusted Cryptography Module (eTCM) and the Embedded System Trusted Platform Control Module (eTPCM), which are combined and implemented the TPM's autonomous control, active defense, high-speed encryption/decryption and other function through its internal bus arbitration module and symmetric and asymmetric cryptographic engines to effectively protect the security of embedded system. In our improved TPM, a trusted measurement method with chain model and star type model is used. Finally, the improved TPM is designed by FPGA, and it is used to a trusted PDA to carry out experimental verification. Experiments show that the trusted architecture of the embedded system based on the improved TPM is efficient, reliable and secure.

1 Introduction

At present, some of traditional information security technologies used by the information system are lack of active defense function [1] to lead to the majority of security problems to lag solving without a unified security system. With the development of Internet of Things (IoT), a variety of embedded systems applications continue to grow such as sensor networks, smart cards, mobile devices, medical, avionics, automotive and smart grid control systems etc. [2]. On one hand, the embedded system is open to the Internet/mobile Internet and it has external attack channels in the IoT. On the other hand, the architecture of embedded systems is too simple and its resource permissions can be arbitrarily used and its executable program is easily included malicious code to control system. So the embedded system may bring security problems. Solving the security of embedded systems is a new challenge in the field of embedded application in the IoT era.

To solve the security of embedded systems in the IoT, it is necessary to improve the architecture and increase the active monitoring and prevention mechanism for the virus or malicious code, and enhance the security of the whole system.

2 Related works

The Trusted Computing Organization (TCG) has proposed a set of trusted computing concepts and methods for the PC information security problem [3], which requires a trusted platform to include the TPM chip as the root of trust for measurement, and then build a trusted chain level by level to extend the trust relationship to the entire PC system to achieve a trusted security computing environment on the entire platform to guarantee the operation of the computing to execute normally.

At present, the trusted concept for expanding embedded and mobile terminal with TPM chip also is proposed [4-6] to solve the growing trusted computing requirement in the field of embedded information security, such as Apostolos et al propose an embedded system hardware architecture capable of providing security and trust along with physical attack protection using trust zone separation [6]. This paper draws lessons from the trusted PC architecture against its shortcomings and improves the original TPM to propose a trusted architecture for the embedded system based on embedded trusted cryptography module (eTCM) with the Chinese cryptosystem, and creates FPGA hardware platform to verify the prototype system of the trusted architecture.

3Trusted embedded system architecture based on improved TPM

Since the embedded system has strict requirements for function, reliability, cost, size and energy consumption, and the original TPM made by TCG has defects which lacks master capability and complexly calculates cryptography (using only RSA but not the use of symmetric cryptography) and so on. Thus, the original

[*] Corresponding author: xswang@sdwu.edu.cn

PTM is not entirely suitable for embedded systems, it is necessary to improve the TPM. In addition to the original functions, the improved TPM should have some new features for embedded systems.

In this paper, we present a trusted embedded computing architecture based on the improved TPM and the Chinese cryptosystem as shown in Figure 1 (a kind of hierarchy). In the architecture, we use a cryptosystem combined with symmetric and asymmetric cryptography to form an embedded trusted cryptographic module (eTCM), and propose the embedded trusted platform control module (eTPCM) based on the cryptosystem as the trust root, and the trust chain of the embedded information system is established to ensure the security of the applications and the critical information.

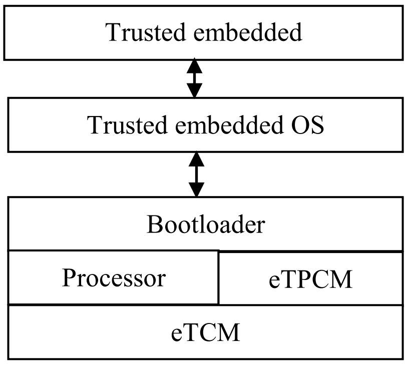

Fig.1. The trusted embedded system architecture based on Chinese cryptosystem.

The eTCM included the cryptosystem is a necessary and critical basic components in the trusted computing platform which provides a support of independent cryptography algorithm. The eTCM includes hardware and firmware that can be integrated with eTPCM in an IP core to serve as an improved TPM.

4 Embedded system trusted platform module

In this paper, an embedded system trusted platform module is designed for embedded systems combining the original TPM and Chinese cryptosystem. The module consisting of the eTCM and the eTPCM is an improvement of the original TPM. The improved TPM has the ability of active control, faster speed of the symmetric encryption and decryption, enhanced the reliability of the system, and supports to achieve chain and star type trust measurement model as a trusted root to effectively reduce the decay and time in the trust transfer. The architecture of the improved embedded system trusted platform module is shown in Figure 2.

According to Chinese trusted computing cryptosystem, the elliptic curve cryptography algorithm used in asymmetric cryptography in eTCM includes three sub-algorithms: digital signature algorithm SM2-1, key exchange protocol SM2-2, public key encryption algorithm SM2-3. The SM4 is used in symmetric cipher algorithm. The SM3 is used in hash algorithm. The cryptographic mechanism uses to protect sensitive data in the system and user sensitive data. The eTPCM is used as a trusted root to provide a series of trusted computing functions such as integrity measurement, safely store, trusted reports, and cryptography services etc. In the eTPCM, a combination of symmetric and non-symmetric cryptography is adopted to improve security and efficiency and active control and measurement are achieved. The bus arbitration module is used to control the main processor in embedded system and the improved TPM access to external memory. i.e. the eTPCM is in the active position due to control the read and write to the external memory and can verify each component in the system separately. A backup memory physically protected is added on the basis of the original TPM to store the boot program and key data of the OS, during they are verified, if they are tampered, it can be easily restored to the external main memory, thus, the reliability of the system is enhanced.

5 The eTPCM trusted measurement protocol

In the paper, a security trust measurement protocol is built with eTPCM as a source of trust for embedded system to achieve the entire hardware and software modules trusted level by level. In the circuit design, the eTPCM is required to start before the embedded main processor so that holds control to the entire circuit system (changing traditional ideas that previous TPM is a passive device). Trusted chain transfer process shown in Figure 3. The specific steps are as follows.

Step 1: Bootloader code is read by the core (RTM) code of the trusted measurement root in the eTPCM, and it is measured, and the report is transferred to the eTPCM. If successful, the control is transferred to Bootloader, go to Step 2. Otherwise, Bootloader code is not trusted, it need to be recovered from the backup memory to be re-measured.

Step 2: Bootloader executes the trusted measurement for embedded OS core code and reports the measurement value to eTPCM. If successful, the OS is loaded and the control is transferred to the OS, go to step 3. Otherwise the OS core code is not trusted and needs to be restored and re-measured.

Step 3: The embedded OS completes the trusted measurement for the trusted service manager, and reports the measurement value to the eTPCM. If successful, the trusted service manager is started. Otherwise, it needs to be restored and re-measured.

Step 4: The trusted service manager completes the trusted measurement of multiple applications that require trusted authentication.

Finally, the trusted service manager resides in the system memory to perform an active measure that measures trust of the applications on runtime from time to time to ensure these applications to be detected timely and remedied after modified by viruses or malicious code.

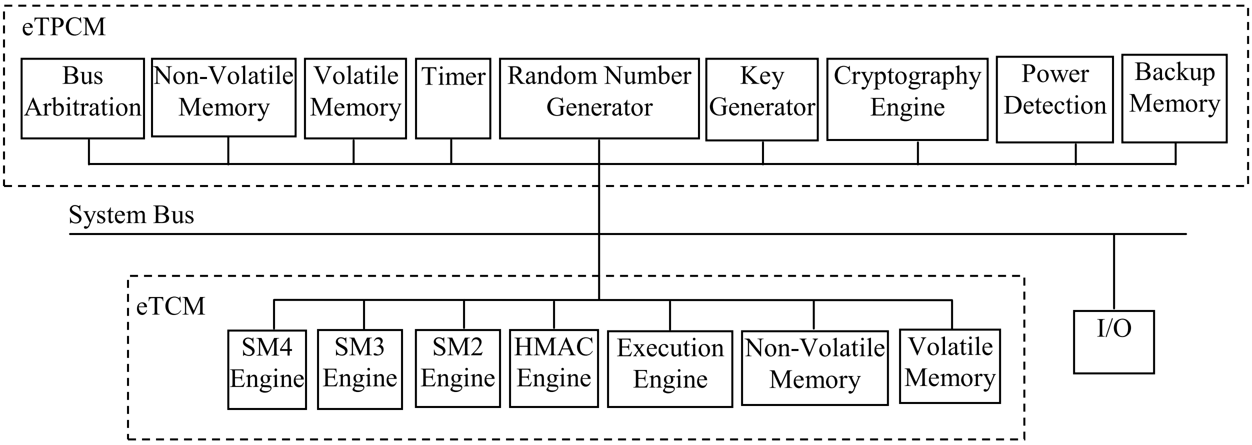

Fig.2. Trusted platform module architecture based on improved TPM for embedded systems.

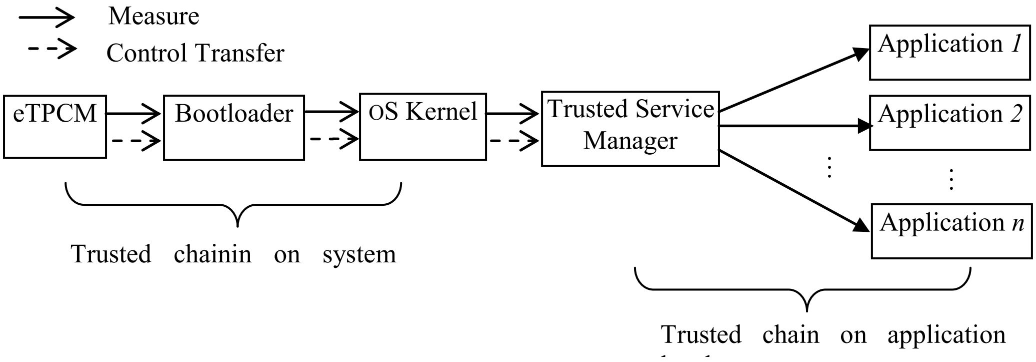

Fig.3. Trusted measurement model of the eTPCM

In the trusted measurement protocol, the chain of trust transfer is combined with chain and star type model. The chain type trusted measurement model is used in the system level and the star type model is used in the application level, which overcomes the defect that only the star type model is used to result in a long measurement due to the eTPCM processor typically performs less. The application is measured by trusted service manager in the user kernel, which is computed by the embedded system host processor, greatly reducing the measurement time.

6 Experimental test and verification

6.1 Verification platform building

In order to validate and evaluate the feasibility and security of the embedded system trusted computing architecture, Altera's Stratix IV E series EP4SE530H40 FPGA is used to perform the improved TPM functionality and apply it to a trusted PDA with ARM processor to complete the test, and a good result is achieved. The prototype system verification platform is shown in Figure 4.

In the start of the trusted PDA, paying attention to the following points:

(1) The improved TPM must be run before power-on and the operation of the ARM processor is controlled by it.

(2) Since the eTPCM to read the external memory data for reliability verification, there are both the ARM processor and the eTPCM need to access the external memory, so the external memory bus needs to be arbitrated.

(3) If you want to upgrade the Bootloader, it must be authorized by eTPCM.

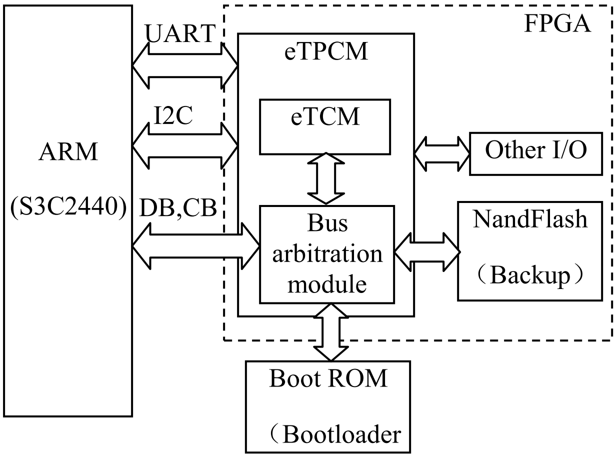

Fig.4. Schematic diagram of improved TPM and trusted PDA prototype verification system

* Corresponding author: xswang@sdwu.edu.cn

In the trusted PDA, the platform acts as a slave and the start-up process of the computer system is controlled by the improved TPM. Before the platform starts, the boot program, the operating system were measured on integrity by the improved TPM and the measurement results of integrity is compared with the values stored previously in the improved TPM to determine whether they are trusted, only the programs that are determined to be trusted can run. If there is an error in the integrity verification process, the improved TPM will automatically call the backup-recovery module to implement the system recovery.

After the system passes the integrity verification, improved TPM allows the ARM processor to run, trusted PDA normal start up to work. During the system executing, the improved TPM is still in the monitoring state, and once the exception is detected it is possible to terminate the trusted PDA reading or writing to the external memory at any time.

From the trusted start-up process of the PDA and the use of the encryption and decryption engine, the improved TPM with the bus arbitration module and the backup- recovery has greatly improved control capability and speeds up the symmetric encryption and decryption.

6.2 Analysis of experimental results

In this experiment, eTPCM needs to perform a trust measurement for the underlying configuration in the starting, and the measurement process can't take too long, if is, although the verification can be completed, but the meaning of the application is lost.

(1) Verifying the embedded system boot program and OS kernel: The verified program size is about 1MB in the experiment, in which boot program is about 60KB and OS kernel is about 800KB. Through the actual verification, entire starting process of experimental system takes less than 0.2s, and the verification speed is nearly 10MB/s, which can meet the requirements of embedded applications.

(2) Testing the speed of the symmetric cryptography encryption and decryption: The symmetric cryptography encryption and decryption engine SM4 is implemented in the hardware of improved TPM, and the execution speed of the engine is up to 7.2MB/s by test. Compared with the 74.6KB/s of the SM4 algorithm that we implemented by software in the PDA, the result of using hardware symmetric encryption and decryption engine greatly improves the encryption and decryption speed.

7Conclusion

This paper proposes a trusted architecture for embedded system from the hardware point of view, and proposes an embedded trusted cryptographic module (eTCM) and an embedded trusted platform control module (eTPCM) based on the Chinese cryptosystem for the architecture. They are combined with each other to complete the improvement of the original TPM. The improved TPM not only conforms to the TCG specification, but also its control over embedded systems is enhanced and it is more compliant with embedded system features. Experiment analysis shows that the design of improved TPM is very effective for embedded systems.

The paper focuses on the improvement of TPM and the functional design in the embedded system environment. The next step is to study the hardware security of improved trusted platform modules.

Acknowledgements

This work has been supported by Project of the Program of The Key Research and Development of Shandong Province, China, under the Grant Numbers 2015GGD01007.

References

1. C.X. Shen, B. Gong. The innovation of trusted computing based on the domestic cryptography. Journal of Cryptologic Research, 2015, 2(5): 381-389.
2. S.L. Keoh, S.S. Kumar, H. Tschofenig. Securing the Internet of Things: A Standardization Perspective. IEEE Internet of Things Journal, 2014, 1(3): 265-275.
3. TCG PC Client Specific TPM Interface Specification (TIS), Specification Version 1.3, 2013.
4. K. Tang, X. Xu, C. Guo. The Secure Boot of Embedded System Based on Mobile Trusted Module, Proceedings of the Second International Conference on Intelligent System Design and Engineering Application, January 6-7, 2012, Sanya: China, IEEE, 2012, 1331-1334.
5. TPM 2.0 Mobile Reference Architecture, Level 00 Revision 142, 2014.
6. Apostolos P. Fournaris, Nicolas Sklavos. Secure Embedded System Hardware Design - A Flexible Security and Trust Enhanced Approach. Computers and Electrical Engineering, 2014, 40(1):121-133.