2015 International Conference on Computational Science and Computational Intelligence

A Study on the Hardware-based Security Solutions for Smart Devices

Hongil Ju, Yongsung Jeon, and Jeongnyeo Kim
Cyber Security System Research Department
Electronics and Telecommunications Research Institute (ETRI)
218 Gajeong-ro, Yuseong-gu, Daejeon, KOREA
juhong@etri.re.kr, ysjeon@etri.re.kr, jnkim@etri.re.kr

Abstract—**For enhanced secure services on smart devices, hardware-based security solutions are required. To this end, the hardware security module is required and it should be physically separated from a smart device. In this paper, we describe the considerations for applying a hardware security module on smart devices. In particular, as smart devices have a limited resource and use a battery, a hardware security module for smart devices should be considered above mobile environment. In this paper, we implemented the hardware security chip for smart devices. In addition, in order to test and equip the implemented chip to a smart device, we implemented the smartphone and verified the secure service on the smart device based on the chip.**

Keywords-hardware secruity module, smart device, security threats, secure service, security chip

I. Introduction

In recent, it is possible to do a lot of things with smart devices such as smartphones due to the advanced various functions. And, the number of smart device's user is gradually increasing because various applications and services deployed on them. With the rapid increasing of mobile services using smart devices, they have contained more and more of the important and sensitive data for above services. In addition, smart devices have been always turned on and connected to the wireless network. As a result, smart devices have become a target of attackers [1], and the security threats on them have caused a serious social issue today. For the continual growth of the smart device market, above issue is one of the problems to be resolved with priority.

To this end, although various security solutions have been implemented and provided, they are almost software-based security solutions. And, most of them have been used on desktop PCs and have been modified for smart devices [2]. As smart devices such as smartphones or smart watches are different from PCs, the mobile-specific security solutions are required. Above all, in order to provide advanced secure service on smart devices, the hardware-based security solutions are required [3]. In addition, as smart devices have limited resources and battery life, the mobile security solutions require lightweight security processing and low power consumption. Therefore, in this paper, we described the hardware-based security solutions for smart devices and implemented the hardware security chip considered above requirements.

The remainder of this paper is constructed as follows. Section II describes related works and Section III shows the implementation of the hardware security module. Finally, we present the conclusions of this paper in Section IV.

II. Related Works

For the hardware-based security solutions, hardware security modules for smart devices are required and there are two kinds of them. One is a security chip integrated with main processor of a smart device. The chip is called System on Chip (SoC) and the TrustZone introduced by ARM [4] is representative. The other is a security chip separated from main processor of a smart device. The chip is called a Secure Element (SE). According to Global Platform, there are three different form factors of SEs, which are a Universal Integrated Circuit Card (UICC), microSD and embedded SE [5]. As an embedded SE is not removable, it is more secure than others. The Trusted Platform Module (TPM) or Mobile Trusted Module (MTM) introduced by Trusted Computing Group (TCG) is one of various embedded SEs. However, it is not easy to apply the embedded SE on smart devices because it should be embedded in manufacturing processing and the smart device should support the space and interface for it. On the other hand, both the UICC and microSD are removable due to the standard interface with smart devices. It means that it is easy to apply both to the existing smart devices without changes of smart devices for the hardware-based security solutions.

III. Implementation of Hardware-based Security Soulutions

For applying a hardware security chip on smart devices, it should be considered that smart devices have limited space and resources compared with PCs. Therefore, the following minimum requirements should be considered.

- The chip size, the power consumption, and the performance overhead due to a security chip should be minimized.
- The separated secure storage, hardware cryptographic co-processors, and cryptographic primitives should be provided.
- The tamper-proof should be provided to protect hardware attacks.

The hardware security chip designed and implemented in this paper has been based on an MTM chip. Therefore, we implemented to support the main functions of an MTM chip

978-1-4673-9795-7/15 $31.00 © 2015 IEEE
DOI 10.1109/CSCI.2015.105

for secure services. Fig. 1 shows the architecture and photograph of the implemented security chip.

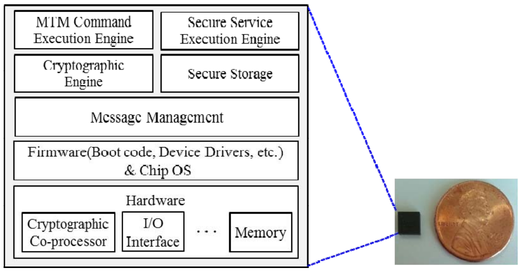

MTM Command Execution Engine
Secure Service Execution Engine
Cryptographic Engine
Secure Storage
Message Management
Firmware(Boot code, Device Drivers, etc.) & Chip OS
Hardware
Cryptographic Co-processor
I/O Interface
. . .
Memory

Figure 1. The arhitecture and photograph of the implemented chip.

As shown Fig. 1, the chip size is 5mm x 5mm, and the chip does not consume more than 10 mA of current. In Fig. 1, "MTM Command Execution Engine" module executes the conventional MTM command messages, and "Secure Service Execution Engine" module executes additional security functions required for secure services. Fig. 2 shows the secure service apps based on the implemented security chip and the implemented smartphone equipped with it.

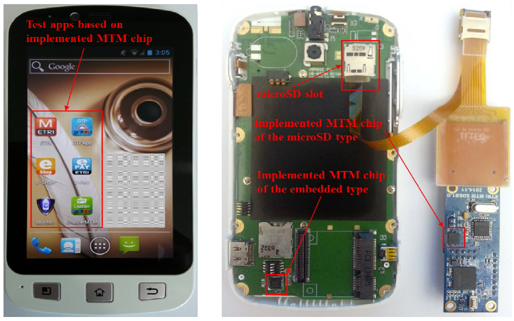

Test apps based on implemented MTM chip
microSD slot
Implemented MTM chip of the microSD type
Implemented MTM chip of the embedded type

Figure 2. The smartphone equipped with the implemented security chip

As shown Fig. 2, the implemented security chip can be embedded directly on a smartphone or can be connected with a microSD interface. And, the smartphone was implemented to apply the security chip to a smart device. For testing and connecting to a microSD slot, we made the evaluation board with the security chip to test and connect to a microSD slot of the smart device. In addition, we designed and implemented additional new commands to support various secure services except conventional MTM commands. Fig. 3 shows the test results of the message exchange for both MTM commands and additional commands.

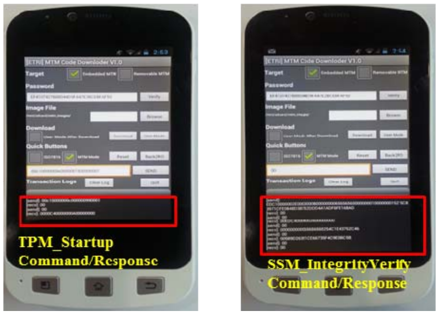
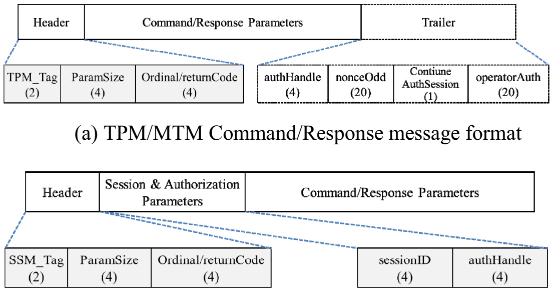

TPM_Startup Command/Response
SSM_IntegrityVerify Command/Response

Figure 3. Test results for message exchange for both commads

In Fig. 3, the "TPM_Startup" message is a MTM command and "SSM_IntegrityVerify" message is one of the additional commands designed and implemented in this paper. As shown Fig. 3, above both messages were executed successfully. Fig. 4 shows the message format of the above.



(a) TPM/MTM Command/Response message format

(b) Additional implemented SSM Command/Response message format

Figure 4. TCG TPM and SSM message format

As shown Fig. 4, unlike (a), we added the "Session & Authentication Parameters" field to manage communication sessions and to access control for the security chip. In addition, according to the value of "SSM_Tag" field, the message can be transferred securely with encryption. In other words, it is possible to establish the secure channel between a hardware security chip and a smart device.

IV. CONCLUSIONS

In this paper, we described the hardware-based security solutions for smart devices. We implemented the hardware security chip and established the secure service execution environment on the smart device using it. In addition, we verified the feasibility of the implemented security chip on smart devices. Therefore, for implementing a hardware security chip, it should be considered the requirements of limited mobile environment, and it is able to reduce the security threats on smart devices. In the future, we are planning to apply the chip to various devices for the Internet of Things (IoT) security services.

ACKNOWLEDGMENT

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) [R-20150518-001267, Development of Operating System Security Core Technology for the Smart Lightweight IoT Devices].

REFERENCES

[1] D. Oh, I. Kim, K. Kim, S. Lee, and W. Ro, "Highly Secure Mobile Devices Assisted with Trusted Cloud Computing Environments" ETRI Journal, vol. 37, no. 2, pp.348-358, Apr. 2015.

[2] X. Zhang, J.P. Seifert, and O. Aciicmez, "Design and Implementation Efficient Integrity Protection for Open Mobile Platforms," IEEE Transaction on mobile coumputing, vol. 13, no. 1, pp.188-201, Jan, 2014.

[3] M. L. Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," IEEE Communications surveys & tutorials, vol. 15, no. 1, pp. 446-471, Mar. 2013.

[4] ARM TrustZone, http://www.arm.com

[5] GlobalPlatform, http://www.globalplatform.org