Supporting a Variety of Secure Services Based on MTM

Seungyong Yoon, Yongsung Jeon
Mobile Security Research Section
Electronics and Telecommunications Research Institute
Daejeon, Rep. of Korea
e-mail: syyoon@etri.re.kr, ysjeon@etri.re.kr

Jeongnyeo Kim
Cyber Security System Research Department
Electronics and Telecommunications Research Institute
Daejeon, Rep. of Korea
e-mail: jnkim@etri.re.kr

***Abstract*—In general, the software security scheme is mainly used to protect the mobile device from the security threat. However, this security scheme can be easily manipulated. For high level of mobile security, it is important to ensure safety and stable service by hardware based security technology such as Mobile Trusted Module (MTM). MTM technology that provides physically enhanced security has been studied. In this paper, we propose a method using a variety of secure services based on MTM technology. Existing e-commerce, authentication, and Digital Rights Management (DRM) services based on MTM technology can improve security and reduced costs.**

Keywords-MTM; secure service; mobile security.

I. INTRODUCTION

The mobile banking and payment services are growing rapidly in recent years. In addition, fraud in mobile financial services is also frequently reported. The initial malware of the mobile device is simply for the purpose of malicious code propagation and paralyzing basic function. Recently, however, malware is evolved into the type of information leakage and financial charge. In particular, mobile malware using 'phishing' and 'smishing' will intentionally cause financial charges to infected users is very prevalent. So, it is proceeding and developing a variety of researches and solutions to prevent damage from mobile attack [1][2].

Generally, because software can be easier exploited than hardware, the researches using hardware-based technique that provides physically enhanced security have been proceeding [3][4].

Mobile Trusted Module (MTM) is one of the solutions to security problems of mobile device. MTM is a security element and a newly approved Trusted Computing Group (TCG) specification for use in mobile and embedded devices [5]. MTM designed to secure hardware by integrating user authentication, platform integrity, device authentication, and data protection to devices for the purpose of blocking information leakage and hacking from mobile device, such as smart phone [6].

MTM basically provides tamper-resistant feature to respond to physical attack. Also, MTM provides a Root of Trust function, Root of Trust for Storage (RTS) for the secure storage of data, Root of Trust for Measurement (RTM), which records the measurement state of system in the MTM, and Root of Trust for Reporting (RTR) to verify the trusted state of the system.

MTM's specification contains a number of functions. However, many functions can be summarized into the following three functions: platform integrity verification, protected storage, and remote attestation. In order to provide these security functions, MTM basically has execution engine, as well as encryption co-processor, random number generator, sha-1/hmac hash engine, key generators, and so on.

In this paper, we propose and implement the method that can provide various MTM-based secure services safely at a lower cost by adding service modules, such as banking, payment, authentication, encryption, and DRM to basic functions of existing MTM's specification.

The rest of this paper is organized as follows. Section II gives an overview of related work and provides a discussion of our contribution. Section III describes secure service provision based on MTM. Section IV describes implementation and operational test, followed by conclusion in Section V.

II. RELATED WORK

MTM is TCG's specifications for trusted computing technologies in mobile devices. There are a lot of researches and studies that relates to MTM. Kim et al. presented design and implementation of a MTM which should satisfy small area and low-power condition [7]. Schmidt et al. proposed how to deploy MTM to a trustworthy operating platform [8]. Dietrich et al. proposed and analyzed existing approaches for providing modular, customizable MTM functionality which are based on currently available cell phones' security extensions [9]. Bugiel et al. introduced a framework for application-specific credentials and provided a prototype implementation using MTM technologies [10].

MTM 2.0 use cases include mobile commerce use cases for mobile banking and payment [11]. However, these mobile commerce services have not been implemented so far. In order to activate prevalent use of a variety of secure services based on MTM, the method using existent MTM function to improve the security must be proposed and implemented. Our proposed method can provide more secure services based on MTM at a lower cost.

III. SECURE SERVICE PROVISION BASED ON MTM

Figure 1 shows the basic architecture of the MTM-based secure service system. Existing traditional MTM command is executed and processed by the MTM execution engine. However, non-traditional MTM command for banking and

 ISBN: 978-1-61208-439-8

payment services is processed and executed in the secure service execution engine.

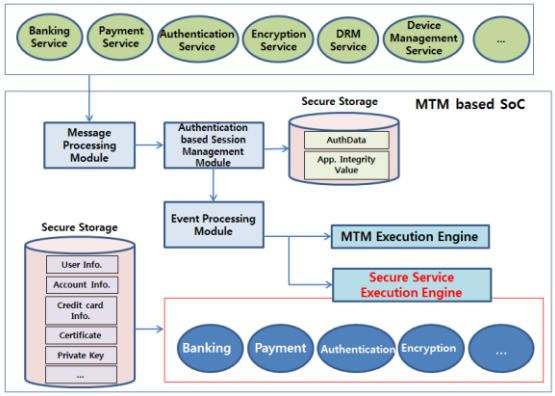

Figure 1. Basic architecture

In order to process two types of commands in the MTM-based security chip, the functional extension of the MTM message processing module is required. In addition, to provide a variety of services safely, it is necessary to have extensions of user authentication and application-based session management module. Secure service execution engine stores important information, such as user information, bank account information, credit card information, certificate, and encryption key in the secure storage. This engine processes the received command, which requests access to information within secure storage.

Conventional TPM/MTM command (Type 1) is used as the field and value defined in the standard specification, and SSM command (Type 2) for the secure service is used as extended header field. According to the 'tag' value of header field, request and response are defined to use for common channel or secure encrypted channel. The 'ssnID' of header field added to support multiple sessions is used to identify and manage the session efficiently.

Figure 2 shows the authentication-based session management module. The 'AuthData' is for user authentication through the 'TakeOwnership' process for a mobile device, and this data is stored in secure storage of MTM security chip. In addition, when an application is installed on a mobile device, 'App Integrity Value' through the application integrity verification process is stored in secure storage.

In order to use the secure services of the MTM, the application tries to establish a session. The session is established only if the 'AuthData' and 'App Integrity Value' comparison process for user authentication and application integrity verification are passed, respectively.

The multi-session support is essential for multiple applications to take advantage of the MTM secure services at the same time. The following values are created and registered in the session table: 'SessionID' to identify each session, 'AuthHandle' value which is dynamically assigned to pass authentication process of the session, and 'SessionKey' value to support the encrypted communication over secure channel.

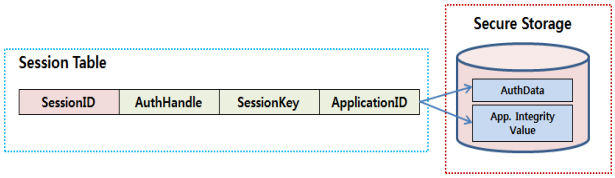

Figure 2. Authentication-based session management module

After the message processing module and the authentication-based session management module, the control comes to the event processing module. The event processing module calls the appropriate function or procedure to execute the command according to the type of command. The secure service execution engine provides a range of secure services, such as banking, payment, authentication, encryption, and DRM service. In addition, this engine stores and manages important information for a service providing to the secure storage and requests and processes the necessary information during command execution.

The command is processed by the secure service execution engine. The various types of service commands are supported: banking, encryption/decryption, integrity verification, device management, payment, sessions and key management, data protection, access control and secure channel, and so on. In addition, other service commands can be extended and defined.

IV. IMPLEMENTATION & OPERATIONAL TEST

We have developed MTM chip for providing secure service, android mobile device embedded MTM chip, and a variety of application using the secure services. Figure 3 shows a screenshot of mobile device embedded MTM chip and secure service applications, such as banking, payments, and device management.

Figure 3. MTM based mobile device and secure service applications

The sensitive personal data stored in existing mobile device was easily leaked when the device was infected by mobile malware. However, the MTM-based secure services using our proposed method in this paper, without leaking personal information, such as banking, payment, and device management, can be provided safely. We have confirmed this safety by operational test.

First, we performed hacking test of commercial smartphone. Most of the mobile malwares are distributed by sending SMS messages or E-mail. We are using E-mail for this test. The mobile malware is downloaded and installed on

 ISBN: 978-1-61208-439-8

user's mobile devices by masquerading as a common normal application. An attacker inserts malicious code into an application. Once the malicious application is installed and run successfully, malicious code collects and steals private data stored in mobile device, for example, SMS messages, contacts list, pictures and digital certificate.

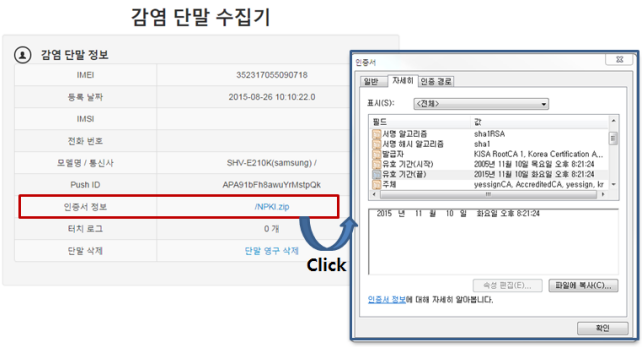

Figure 4. Screenshot of hacker's server

In the hacker's screen from Figure 4, 'NPKI.zip' is a digital certificate. By clicking on the link, we can get more detailed information. This certificate is very important and sensitive private data which is widely used in field of mobile e-commerce in Korea. Digital certificate can be easily leaked from commercial device.

On the other hand, in case of our proposed method, there is no digital certificate on hacker's server in the same test. Because digital certificate is protected securely within secure storage of MTM hardware, hacker failed to get this private data.

V. CONCLUSION

In this paper, we proposed a method using a variety of secure services based on MTM technology. Our proposed method, utilizing existent MTM function to improve the security, can provide more secure services at a lower cost. In addition, the proposed method has a scalability to support a wide range of additional secure services to meet the needs of users.

ACKNOWLEDGMENT

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.R-20150518-001267, Development of Operating System Security Core Technology for the Smart Lightweight IoT Devices).

REFERENCES

[1] Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution", IEEE Symposium on Security and Privacy, 2012, pp. 95-109.

[2] M. Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices", IEEE Communications Surveys & Tutorials, vol. 15, 2013, pp. 446-471.

[3] Trusted Computing Group (TCG), "TPM Main Specification Version 1.2, Revision 116", Mar. 2011.

[4] G. Cabiddu, E. Cesena, R. Sassu, D. Vernizzi, G. Ramunno, and A. Lioy, "The Trusted Platform Agent," IEEE Software, vol. 28, 2011, pp. 35-41.

[5] Trusted Computing Group (TCG), "Mobile Trusted Module Specification Version 1.0, Revision 6", Jun. 2008.

[6] J. Ekberg and M. Kylanpaa, "Mobile trusted module (MTM) - an introduction", Nokia Research Center, Nov. 2007.

[7] M. Kim, H. Ju, Y. Kim, J. Park, and Y. Park, "Design and Implementation of Mobile Trusted Module for Trusted Mobile Computing", IEEE Transaction on Consumer Electronics, vol. 56, Feb. 2010, pp. 134-140.

[8] A. Schmidt, N. Kuntze, and M. Kasper, "On the deploy of Mobile Trusted Modules", IEEE Wireless Communications and Networking Conference, Mar. 2008, pp. 3169-3174.

[9] K. Dietrich and J. Winter, "Towards Customizable, Application Specific Mobile Trusted Modules", ACM Workshop on Scalable Trusted Computing, 2010, pp. 31-40.

[10] S. Bugiel and J. Ekberg, "Implementing an Application-Specific Credential Platform Using Late-Launched Mobile Trusted Module", ACM Workshop on Scalable Trusted Computing, 2010, pp. 20-30.

[11] Trusted Computing Group (TCG), "Mobile Trusted Module 2.0 Use Cases", Mar. 2011.

 ISBN: 978-1-61208-439-8