http://dx.doi.org/10.14400/JDC.2016.14.11.501

HW기반 스마트 단말 보안 핵심기술 구현

김정녀
한국전자통신연구원

Security Core Technology Implementation for Hardware-based Smart Devices

Jeong Nyeo Kim
Electronics and Telecommunications Research Institute

요 약 최근 들어, 스마트 단말에서 지불, 인터넷 뱅킹 등 금융업무와 관련된 중요한 정보들을 다루는 경우가 많아졌다. 또한 스마트 단말의 실행환경이 공개 소프트웨어 환경 위주로 발전하면서, 사용자들이 임의의 응용소프트웨어를 다운받아 사용하는 것이 용이하게 됨에 따라, 스마트 단말이 보안적 측면에서 취약하게 되었다. 본 논문에서는 하드웨어 기반의 스마트 단말 보안 기술의 특징을 알아본다. 또한, 본 논문에서는 스마트 단말 에서 실행되는 응용프로그램을 위한 MTM 하드웨어기반의 안전한 스마트 단말 실행환경에 대한 구현방법을 제안한다. 기존의 MTM 이 모바일 장치에 대한 신뢰의 근원 기능만을 제공한 반면, 본 논문에서 제시하는 MTM 기반 모바일 보안 환경은 모바일 장치에서 실행되는 응용프로그램이 필요로 하는 다양한 보안 기능을 제공할 수 있다. 향후, 보안 하드웨어와 연동이 가능한 IoT 기기와 게이트웨이 보안 기술, 그리고 보안 하드웨어를 활용하여 다양한 IoT 기기에 적용하여 신뢰성과 보안성을 확보하는 방안에 대한 연구를 진행할 예정이다.

주제어 : 스마트 단말 보안, 모바일 신뢰 모듈, 무결성 검증, 인터넷 뱅킹, 보안 관리

Abstract Recently, the frequency of dealing important information regarding financial services like paying through smart device or internet banking on smart device has been increasing. Also, with the development of smart device execution environment towards open software environment, it became easier for users to download and use random application software, and its security aspect appears to be weakening. This study inspects features of hardware-based smart device security technology. Furthermore, this study proposes a realization method in MTM hardware-based secure smart device execution environment for an application software that runs in smart devices. While existing MTM provides the root of trust function only for the mobile device, the MTM-based mobile security environment technology proposed in this paper can provide numerous security functions that application program needs in mobile device. The further researches on IoT devices that are compatible with security hardware, gateway security technology and methods that secure reliability and security applicable to varied IoT devices by advancing security hardware are the next plan to proceed.

Key Words : Smart Device Security, Mobile Trusted Module, Integrity Verification, Internet Banking, Security Management

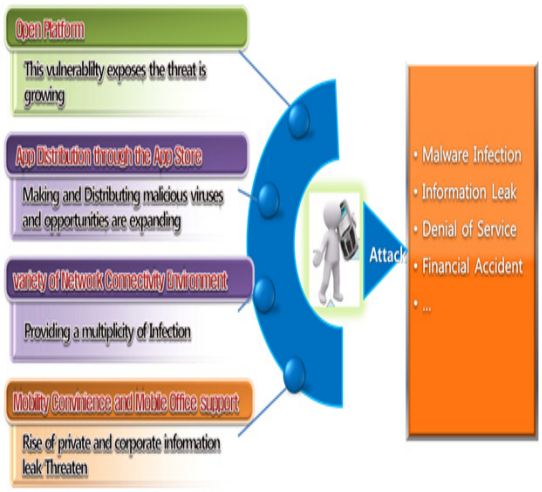
* 이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(B0190-16-2032, 스마트 경량 IoT 기기용 운영체제 보안 핵심 기술 개발)
Received 28 September 2016, Revised 31 October 2016
Accepted 20 November 2016, Published 28 November 2016
Corresponding Author : Jeong Nyeo Kim
(Electronics and Telecommunications Research Institute)
Email: jnkim@etri.re.kr

ISSN: 1738-1916

1. Introduction

Expansion of new mobile threatens like privacy infringement, mobile malware and etc. is expected as smart devices are rapidly spreading. Especially the worm virus that runs in mobile device like smartphone might cause performance degradation of mobile device, illegally collecting personal information of mobile device users, virus spreads to other services and etc., and thus it is crucial to provide against those threatens. Concerns that in case of lost or stolen of the mobile device, leak of information stored internally in mobile device and copy of mobile are rising. In addition, as open mobile platform market preference is increasing also the possibility of mobile device open platform like Android might be targeted for hacking attack. Along with service expansion focusing on open platform for smart device, software-based solutions like Anti-Virus against increasing security threatens are limited and security policy like MDM or similar level application service cannot prevents damages from leak of internally stored significant information when smart device is rooted without user knowing. Domestic smart device security technologies are composed with application level single configuration techniques like Anti-virus, Firewall function, Device interlock and others which are relatively the beginning stage of technology. [1] TCG (Trusted Computing Group) presented a hardware security module MTM which is compatible in mobile environment.

MTM installed in mobile device equipping with various security functions including platform integrity verification function, occlusion area, protection, safe key control, physical security and so on provides an environment that processes and manages files used on the inside of device and verifies integrity of device platform[3, 4]. Considering the features of smart device like low power, low capacity, multimedia service, execution environment, etc., developing certain level of system and secure platform technology are top priority before anything else to protect smart device in open platform environment from numerous security threatens mentioned above. On this research paper, MTM hardware-based security technology implementation that provides security function in platform level for smart device will be studied.



[Fig. 1] Smart device security threaten

2. Smart Device Security Threaten

Security threatens in smart device can be roughly categorized into four sections. First, This vulnerability exposes the threat is growing as an open platform. Second, Depending on the application distribution through the App Store making and distributing malicious viruses and opportunities are expanding. Third, It supports a variety of network connectivity environment providing a multiplicity of infection. Last, a rise of private and corporate information leak threaten from mobility convenience and mobile office program.

The damages are also continued to go on to infection of malware, leak of private/corporate information, denial of service attack, financial accident and so on. Worldwide mobile malware infection routes are Bluetooth 76.1%, MMS 24.4%, External storage device

3.7%, PC plug-in 2.4%, Internet download 2.4% and etc. Platform security technology is significant to protect smart device from various security threatens like these.

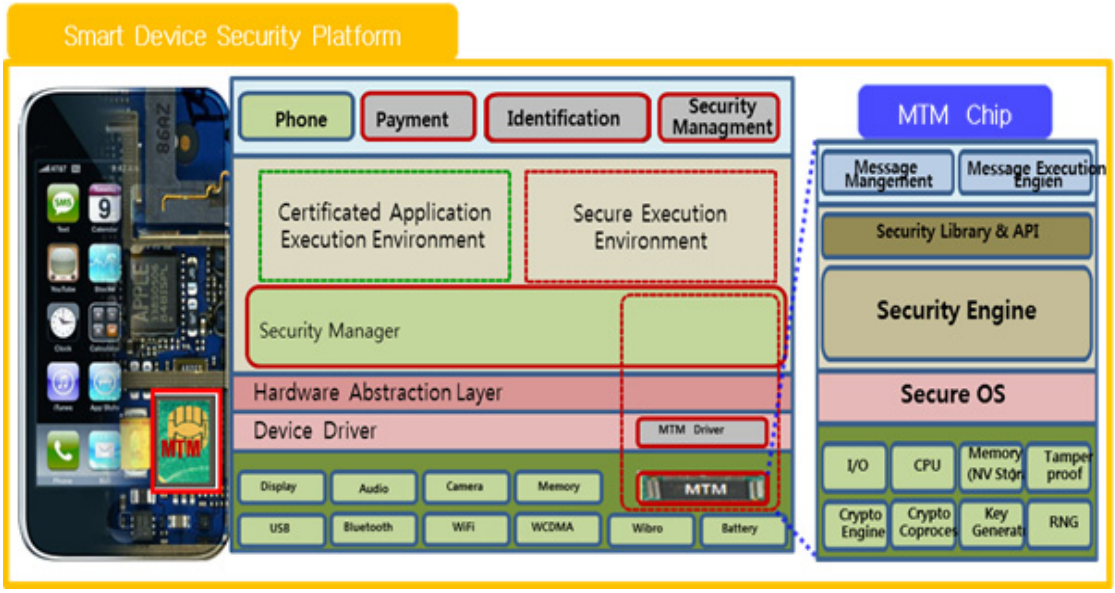
3. Security Technology Implementation Of MTM-Based Smart Device

As mentioned above, MTM is a root of trust module in mobile device.

MTM provides three roots of trust on mobile device; RTS (Root of Trust for Storage), RTM (Root of Trust for Measurement), RTR (Root of Trust for Reporting). However, existing MTM is not providing protection function at important information used in application program in mobile device. Thus, the need for MTM to provide diverse security functions for application programs that used in mobile device is rising. This research proposes MTM-based secure execution environment that can protect important information in mobile device as you can see in [Fig. 2] This secure execution environment for mobile device can provide various MTM-based security functions for application programs in mobile device.

4. Implementation And Test Result

Most of the mobile malwares are infected by sending SMS messages or email. Mobile malwares are usually downloaded and installed in user's smart device pretending it is just a normal application. The attacker inserts malware into application then the application is installed and executed. The malware collects and takes the sensitive data like messages, phonebook, picture, authentication certificate from smart device. This technology prevents information leak from smart device and detects mobile malware infection. As soon as when the mobile malware is run in MTM, the security module will detects it and warn user. Detection report will be sent to MDM (Mobile Device Management Server) also. The green light will be changed to red on MDM screen. In case of mobile vaccine, software-based security solution cannot detect changes from access-allowed system library. Mobile



[Fig. 2] Proposed MTM-based mobile security execution environment

[Fig. 3] Detection test of mobile malware

vaccine also fails to detect new mobile malware because the malware patterns are not existed in DB. This technology is capable of detecting system level attacks as well as new mobile malware. Integrity verification test to detect malware will be done. Security module measures the original value integrity inside of MTM hardware. Alarm messages will be generated when these values are modified illegally.

5. Conclusion

This research paper examined hardware-based security technologies which are needed in smart mobile device. While existing MTM provides the root of trust function only for the mobile device, the MTM-based mobile security environment technology proposed in this paper can provide numerous security functions that application program needs in mobile device. MTM-hardware-based mobile device security technology precludes the leak of sensitive information and unauthorized access. This technology will be a solution that prevents spreading and executing of malware not only in smart devices but in different field including many different IoT devices on internet. As various and new IoT services are appeared, an escalation of communicating and connecting between devices that has a number of features and specification is expected. Service security enhancement and secure service environment establishment must be accompanied with this changing situation to respond approaching various security threatens because of features of these IoT service environments. The further researches on IoT devices that are compatible with security hardware, gateway security technology and methods that secure reliability and security applicable to varied IoT devices by advancing security hardware are the next plan to proceed.

ACKNOWLEDGEMENT

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant

funded by the Korea government(MSIP) (B0190-16-2032, Development of Operating System Security Core Technology for the Smart Lightweight IoT Devices)

REFERENCES

[1] Mobey Forum Mobile Financial Services, " Alternatives for Banks to offer Secure Mobile Payments version 1.0," Aug. 2010.

[2] TCG mobile reference architecture specification version 1.0, (https://www.trustedcomputinggroup.org)

[3] Siani Pearson, "Trusted Computing Platforms", 2003.

[4] TCG, "TCG Mobile Trusted Module Specification. Version 1.0, Revision 7.02, April 28, 2010

[5] S. Choi, J. Han, J. Lee, J. Kim, S. Jun, "Implementation of a TCG-based trusted computing in mobile device", TrustBus 2008 pp.18-27

[6] "TrustZone API Specification" Version 3.0, ARM, February 2009.

[7] "TEE Client API Specification" Version 1.0, Global Platform, July 2010.

[8] Global Platform site, http://www.globalplatform.org/specifications device.asp

[9] "TEE System Architecture" Version 1.0, Global Platform, December 2011.

[10] Keun-Ho Lee, "A Security Threats in Wireless Charger Systems in M2M", Journal of the Korea Convergence Society, Vol. 4, No. 1, pp. 27-31, 2013.

[11] Sik-Wan Cho, Won-Jun Jang, Hyung-Woo Lee, "Development of User Oriented Vulnerability Analysis Application on Smart Phone", Journal of the Korea Convergence Society, Vol. 3, No. 2, pp. 7-12, 2012.

[12] Seong-Gwon Yeo, Keun-Ho Lee, "Smart Phone and Vehicle Authentication Scheme with M2M Device", Journal of the Korea Convergence Society, Vol. 2, No. 4, pp. 1-7, 2011.

[13] Keun-Ho Lee, "Analysis of Threats Factor in IT Convergence Security", Journal of the Korea Convergence Society, Vol. 1, No. 1, pp. 49-55, 2010.

[14] Seong-Ryeol Kim, "Design of a User Authentication System using the Device Constant Information", Journal of IT Convergence Society for SMB, Vol. 6, No. 3, pp. 29-35, 2016.

[15] Hyung-Jin Mun, Gwang-Houn Choi, Yooncheol Hwang, "Countermeasure to Underlying Security Threats in IoT communication", Journal of IT Convergence Society for SMB, Vol. 6, No. 2, pp. 37-44, 2016

김 정 녀(Kim, Jeong Nyeo)

- 1987년 2월 : 전남대학교 전산통계학과(이학사)
- 1996년 5월 : OSF/RI 공동연구 파견(미국)
- 2004년 2월 : 충남대학교 컴퓨터공학과(공학석사, 공학박사)
- 2005년 1월 : Univ. of California, Irvine Post-Doc (미국)
- 1988년 2월 ~ 현재 : 한국전자통신연구원 책임연구원
- 2015년 3월 ~ 현재 : 과학기술연합대학원대학교(UST) 정보보호공학과 교수
- 관심분야 : IoT보안, 모바일 보안, 시스템·네트워크보안, 보안 OS 등
- E-Mail : jnkim@etri.re.kr