Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.6, Dec. 2016 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2016.26.6.1455

MTM하드웨어 기반 스마트 단말 보안 핵심기술 구현*

김 정 녀†‡
한국전자통신연구원 모바일보안연구실

Security Core Technology Implementation for MTM 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 단말에서 실행되는 응용프로그램을 위한 MTM(Mobile Trusted Module) 하드웨어기반의 안전한 스마트 단말 실행환경에 대한 구현방법을 제안한다.

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 will inspect features of hardware-based smart device security technology. Furthermore, this study will propose a realization method in MTM hardware-based secure smart device execution environment for application software runs that in smart device.

Keywords: Smart Device Security, Mobile Trusted Module, Integrity Verification

I. 서 론

스마트 단말의 보급이 급격하게 증가하고 있는 현실에서 모바일 환경에 대한 개인정보 침해, 모바일 악성코드 등 새로운 모바일 위협의 확대가 예상되고 있다. 특히, 스마트폰 등 모바일 장치에서 실행되는 웜, 바이러스는 모바일 장치의 성능저하, 모바일 사용자의 개인 정보 불법 수집, 다른 서비스로의 바이러스 전파 등을 야기시킬 수 있어 이에 대한 대비가 무엇보다 중요하다. 또한, 모바일 장치의 도난/분실 시 모바일의 복제, 모바일 장치 내부에 저장된 정보의 유출에 대한 우려가 제기되고 있다. 뿐만 아니라, 개방형 모바일 플랫폼에 대한 시장 선호도가 높아짐에 따라 안드로이드와 같이 모바일 장치의 개방형 플랫폼이 주요 해킹의 표적이 될 가능성이 많아지고 있다. 이와 같이, 스마트 단말에 대한 개방형 플랫폼을 중심으로 하는 서비스 확대와 함께 보안 위협의 증대는 Anti-Virus 와 같은 기존 소프트웨어 기반 솔루션으로는 대응에 한계가 있으며, MDM(Mobile

Received(10. 12. 2016), Modified(11. 25. 2016), Accepted(11. 26. 2016)
* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발 사업의 일환으로 하였음(B0190-16-2032, 스마트 경량 IoT 기기용 운영체제 보안 핵심기술 개발)
† 주저자, jnkim@etri.re.kr
‡ 교신저자, jnkim@etri.re.kr(Corresponding author)

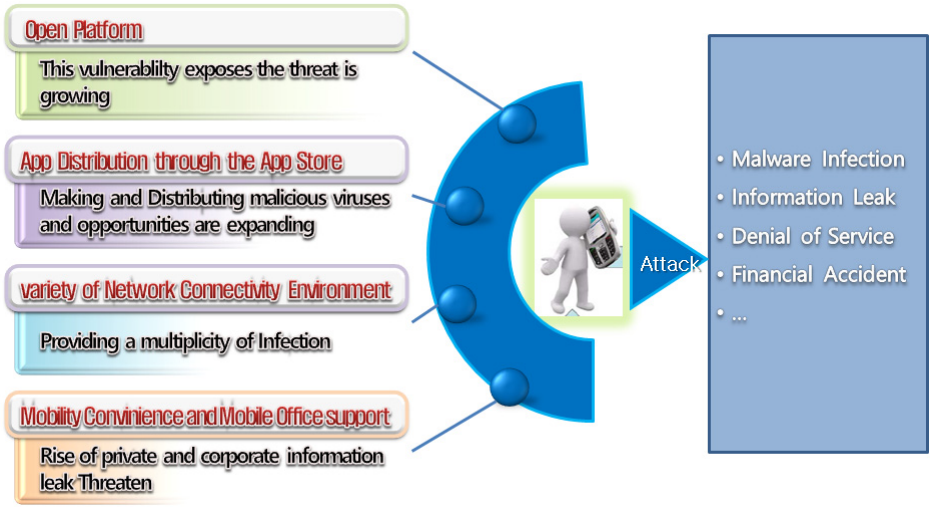

Fig. 1. Smart Device Security Threaten

Device Management, 이하 MDM) 과 같은 응용서비스 수준의 보안 대책으로는 사용자가 모르는 상태에서 스마트 단말이 루팅되어 내부의 중요한 정보가 유출되는 등의 피해에 대해서는 방지를 할 수가 없다. 특히, 국내 스마트 단말 보안 기술은 안티 바이러스, 방화벽 기능, 디바이스 잠금 기능 등과 같은 어플리케이션 수준의

단품형 기술로 구성되어 있으며, 비교적 초기 단계의 기술이라고 할 수 있다[1] TCG (Trusted Computing Group)에서 모바일 환경에 적합한 하드웨어 보안 모듈인 MTM(Mobile Trusted Module, 이하 MTM) 을 발표하였다.

MTM은 모바일 단말에 장착되어 단말 자체에 대한 플랫폼 무결성 검증 기능은 물론 차폐영역과 보호능력 및 안전한 키관리 체계, 물리적인 안전성 등 다양한 보안기능을 제공하기 때문에 단말 플랫폼의 무결성 검증 및 단말내부에서 사용되는 파일들을 안전하게 처리하고 관리해 줄 수 있는 환경을 제공한다[3][4]. 스마트 단말의 저전력, 저용량, 멀티미디어 서비스, 실행 환경 등의 특성을 고려하여, 위에서 언급한 다양한 보안 위협으로부터 개방형 플랫폼 환경의 스마트 단말을 보호하기 위한 시스템 수준의 보안 플랫폼 기술 개발이 최우선적으로 요구되고 있다. 본 논문에서는 스마트 단말에 대하여 플랫폼 수준의 보안 기능을 제공하는 MTM 하드웨어 기반의 보안 기술의 구현에 대해 알아본다.

II. 스마트 단말 보안 위협

스마트 단말에서의 보안 위협은 그림 1.과 같이 크게 네 가지로 나눌 수 있다. 첫째는 개방형 플랫폼으로 진화됨에 따라 보안 취약점 노출위협이 증대되고, 두 번째는 앱스토어를 통한 애플리케이션 유통 구조에 따라 악의적인 바이러스 제작 및 유포 기회가 확대되고 있으며, 세 번째는 다양한 유·무선 네트워크 접속환경을 지원하고 있어 감염경로의 다양성을 제공하며, 마지막으로 이동 편의성 및 모바일 오피스 지원에 의해 개인 및 기업 정보 유출 위협이 크게 증대한다는 것이다.

그 피해 또한 악성코드 감염, 기업/개인정보 유출, 서비스 거부 공격, 금융사고 등으로 이어지고 있다. 특히 잘 알려지지 않은 악성코드에 감염되는 것을 통해 스마트 단말의 제어권을 획득하는 등의 새로운 공격의 시도는 지속적으로 시도되고 있다.

전 세계 모바일 악성코드 감염경로 비율을 보아도 블루투스 67.1%, MMS(24.4%), 외부저장장치(3.7%), PC플러그인 (2.4%), 인터넷 다운로드(2.4%) 등으로 이루어진다. 이러한 다양한 보안 위협으로부터 스마트 단말을 보호하기 위해 플랫폼 보안 기술이 필요하다.

III. 스마트 단말 보안 기술 구현

앞에서 언급한 바와 같이, 아래 그림 2의 중앙에

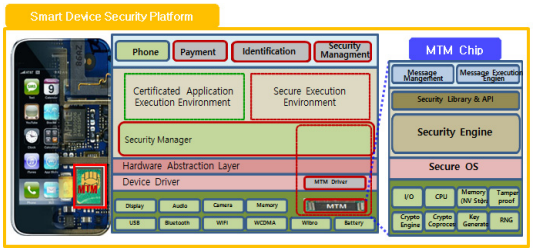

Fig. 2. Proposed MTM-based mobile security execution environment

있는 MTM은 모바일 장치에 있어서 마스터키를 저장하여 신뢰 루트(Root of trust) 기능을 제공하는 모듈이다. 스마트 단말에서는 MTM을 구동하는 디바이스 구동기와 하드웨어 추상화 계층, 그리고 보안 관리 등이 구현되었으며, 실제 MTM보안 모듈에서는 보안 OS, 그리고 보안 실행 엔진 그리고 보안 관리 API 등이 구현되어 스마트 단말 보안 플랫폼 기능을 제공한다.

MTM 은 모바일 장치에 대하여 다음과 같은 3가지의 신뢰 루트(Root of Trust) 기능을 제공한다. 즉, RTS(Root of Trust for Storage), RTM(Root of Trust for Measurement), RTR(Root of Trust for Reporting). 그러나 기존의 MTM 은 모바일 장치에서 실행되는 응용 프로그램이 실행되는 서비스 환경에 대한 안전 실행 환경은 제공하지 못하고 있다. 따라서 MTM도 모바일 장치에서 실행되는 응용 프로그램이 필요로 하는 다양한 보안 기능을 제공할 필요성이 대두되고 있다.

본 논문에서는 그림 2 와 같이 모바일 장치에서의 중요한 정보를 보호할 수 있는 MTM 기반의 안전한 실행환경을 제안한다. 이 모바일 장치용 안전 실행환경은 모바일에서 실행되는 응용프로그램을 위하여 MTM 기반으로 다양한 보안 기능을 제공할 수 있다. 사용자의 중요한 데이터나 민감한 처리 들은 MTM에서 실행되는 보안 API를 통하여 MTM 하드웨어에서 실행되게 함으로써 안전한 실행 환경을 제공한다. 예를 들면, 인증서와 같이 민감한 데이터를 처리하는 경우에는 MTM에서 실행되는 보안 API를 통하여 MTM의 보안 OS와 보안 엔진에서 처리 될 수 있도록 하는 MTM 기반의 안전 실행 환경을 지원한다.

IV. 구현 및 테스트 결과

MTM기반 스마트 단말 보안 플랫폼은 그림 3과 같이 구현하였다. 1차는 단말 플랫폼과 MTM칩 테스트 보드로, 2차는 단말 플랫폼과 MTM칩을 연동하는 플랫폼으로, 마지막에는 단말 플랫폼을 제작하여 단말 내에 MTM칩을 장착하는 시제품으로 제작하여 연동 작업을 완료하였다.

대부분의 모바일 악성코드는 SMS 메시지나 이메일을 보내는 것으로 감염된다. 모바일 악성코드는 보통 정상적인 앱처럼 가장하여 사용자의 스마트 단말에 다운로드 되고 설치된다. 공격자는 앱에 악성코드를 삽입하여, 악성 앱이 성공적으로 설치되고 실행된다. 악성코드는 SMS 메시지, 주소록, 그림, 인증서 등과 같은 스마트 단말 내의 민감 데이터를 수집해서 가져간다. 특별히 인증서는 국내에서 모바일 뱅킹이나 지불에 널리 쓰이는 가장 중요하고 민감한 데이터이다.

본 기술은 그림 4.에서 나타내는 바와 같이 스마트 단말로 부터의 정보 유출을 방지하고 모바일 악성

Fig. 3. MTM-based Smart Device Platform Prototype

Fig. 4. Detection test of mobile malware

코드 감염을 탐지한다. 악성코드에 의해 이미지의 무결성을 탐지하는 것은 크게 두 단계로 나누어서 볼 수 있다. 첫 번째 단계는 부팅시점과 커널 모듈 로딩 시점에 변조된 이미지를 탐지하는 정적 무결성 검증(Static Root of Trust) 단계로 커널 모듈, 시스템 라이브러리 로딩 단계인 부팅 시점에 각 이미지의 무결성을 측정하고 검증하는 단계이며, 두 번째 단계는 커널 모듈과 시스템 라이브러리가 악성코드에 의해 변경되는 시점에서 탐지하는 동적 무결성 검증(Dynamic Root of Trust) 단계로 해킹 앱이나 악성 앱에 의한 시스템 컴포넌트가 변조되는 것을 탐지하여 시스템의 이상 상태를 탐지한다.

본 기술은 모바일 악성코드가 MTM에서 실행되자마자, 무결성을 측정하고 검증하는 보안 모듈이 커널 모듈과 시스템 라이브러리의 변조를 탐지하여 관리자 또는 사용자에 알린다. 이에 대한 탐지 보고를 MDM 서버에게 보내 악성코드에 의해 시스템 무결성이 훼손되었음을 알린다. 이렇듯 모바일 악성코드가 탐지 되는 경우에는 그림 4에서처럼 MDM 화면에 그린 등이 붉은 색으로 바뀌는 것을 볼 수 있다. 기존 모바일 백신의 경우인 응용 수준의 SW기반 보안 솔루션은 접근이 허용된 시스템 라이브러리의 변경을 탐지할 수 없다. 또한 모바일 백신은 알려지지 않은 악성코드의 패턴이 DB에 존재하지 않기 때문에 새로운 패턴의 모바일 악성코드를 탐지 할 수 없다. 그러나 본 기술은 모바일 악성코드 탐지를 위하여 단말 실행 중에 동적 무결성 측정 및 검증을 함으로써 새로운 모바일 악성코드는 물론 시스템 수준의 공격을 탐지할 수 있다. 이러한 MTM기반 무결성 측정 및 검증 보안 모듈이 MTM하드웨어 내에 원래의 값에 대한 무결성을 측정하고 검증하며, 해당 값들이 불법적으로 변경될 때 알람 메시지도 생성한다.

V. 결 론

본 논문에서는 스마트 모바일 장치에서 필요로 하는 하드웨어 기반의 보안 기술들에 대해 알아보았다. 또한, 기존의 MTM이 모바일 장치에 대한 신뢰의 근원(Root of Trust) 기능만을 제공하는 반면, 본 논문에서 제시하는 MTM기반 스마트 단말 보안 환경은 모바일 장치에서 실행되는 응용프로그램이 필요로 하는 다양한 서비스가 안전하게 실행될 수 있는 보안 기능을 제공한다. 본 MTM하드웨어 기반 스마트 단말 보안 기술은 인증서 처리, 인터넷 지불/뱅킹 등과 같은 다양한 서비스 상에서 안전한 실행 환경을 제공함으로써 인증서 등과 같은 민감정보 유출과 비인가 사용자의 접근을 차단한다. 또한 이 기술은 스마트 단말뿐만 아니라 인터넷 상의 다양한 IoT 기기를 포함한 다양한 분야에서 악성코드의 실행과 전파를 막을 수 있는 솔루션이 될 것이다. 다양하고 새로운 IoT 서비스가 등장하면서 여러 가지 사양과 특성을 갖는 수많은 기기 간의 연결과 통신의 증가가 예상되고 있다. 이러한 IoT 서비스 환경의 특성으로 인해 발생 가능한 다양한 보안 위협에 대응하기 위해 안전한 서비스 환경 구축 및 서비스의 보안성 강화는 반드시 수반되어야 한다. 향후, 보안 하드웨어와 연동이 가능한 IoT 기기와 게이트웨이 보안 기술과, 보안 하드웨어를 활용하여 다양한 IoT 기기에 적용하여 신뢰성과 보안성을 확보하는 방안에 대한 연구를 진행할 예정이다.

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”, Prentice Hall PTR Upper Saddle River, 2002
[4] TCG, “TCG Mobile Trusted Module Specification. Version 1.0, Revision 7.02, April 28, 2010.

〔5〕 H.I. Joo, S.G. Choi, S.I. Jeon, "Secure Booting using TPM on Mobile Platform", NCS2006, Dec. 2006.
〔6〕 M.S. Kim, J.A. Shin, Y.S. Park, S.I. Jeon, "Common Security Core Module for Mobile Platform," KIISC, Vol.16, No 3, Jun. 2006.
〔7〕 H. Chai, Z. Lu, Q. Meng, J. Wang, X. Zhang, Z. Zhang, "TEEI-A Mobile Security Infrastructure for TEE Integration, "Proceedings of IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 914-920, Sep. 2014.
〔8〕 M. Kim, H. Ju, Y. Kim, J. Park, Y. Park, "Design and implementation of mobile trusted module for trusted mobile computing," IEEE Transactions on Consumer Electronics, Vol. 56, No. 8, pp. 134-140, Jan. 2010.
〔9〕 K. H. Baek, " Trend of Research and Technology for SEE," Electronics and Telecommunications Trends, Vol 22, No 5, Oct. 2007.
〔10〕 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.
〔11〕 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.
〔12〕 W. Arthur and D. Challener, A Practical Guide to TPM 2.0: Using the Trusted Platform Module in the New Age of Security, Apress, 2015.
〔13〕 Digital Times, "'Micro SD' Adoption for Standard Mobile Payment," 2012.(http://www.dt.co.kr/contents.html?article_no=2012 102502010151741003)

〈저자소개〉

김 정 녀 (Jeong Nyeo Kim) 종신회원
1987년: 전남대학교 전산통계학과 학사
1996년: OSF/RI 공동연구 파견(미국)
2004년: 충남대학교 컴퓨터공학과 석사, 박사
2005년: Univ. of California, Irvine Post-Doc.
현재: 한국전자통신연구원 정보보호연구본부 모바일보안연구실 책임연구원
현재: 과학기술연합대학원대학교(UST) 정보보호공학과 교수
〈관심분야〉 IoT보안, 모바일 보안, 시스템·네트워크보안, 보안 OS 등