http://dx.doi.org/10.14400/JDC.2016.14.12.471

Implementation of Domain Separation-based Security Platform for Smart Device

Jeong Nyeo Kim
Electronics and Telecommunications Research Institute

안전한 스마트 단말을 위한 도메인 분리 기반 보안 플랫폼 구현

김정녀
한국전자통신연구원

Abstract Recently, important information related with smart work such as office and video conference are handled in smart device quite a lot compare with before. Also, execution environment of smart devices is getting developed as open software environment. It brought convenience to download and use any kind of application software. By that, security side of smart devices became vulnerable. This paper will discuss characteristics of smart device security technology based on virtualization that is a mobile device platform with isolated secure execution area based on TEE (Trusted Execution Environment). Also, this paper will suggest an implementation method about safe smart device security platform based on domain separation for application software which can be executed in smart devices. The domain separation based smart device security platform technology in this paper blocks unauthorized access and leakage of sensitive information in device. Also it will be the solution can block transmission and execution of malicious code in various area including variety of IoT devices in internet rather than just smart devices

Key Words : Smart Device Security, Virtualization, Domain Seperation, Trusted Execution Environment, Trusted Military Zone, Smartwork

요 약 최근 들어, 스마트 단말에서 오피스, 화상회의 등 스마트워크 업무와 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 TEE(Trusted Execution Environment) 기반의 격리된 안전실행환경 영역을 가지는 모바일 단말 플랫폼인 가상화 기반 스마트 단말 보안 기술의 특징을 알아본다. 또한, 본 논문에서는 스마트 단말에서 실행되는 응용프로그램을 위한 도메인 분리 기반의 안전한 스마트 단말 보안 플랫폼에 대한 구현방법을 제안한다. 본 논문의 도메인 분리 기반 스마트 단말 보안 플랫폼 기술은 단말내의 민감 정보 유출과 비인가 접근을 차단한다. 또한 이 기술은 스마트 단말 뿐만 아니라 인터넷 상의 다양한 IoT를 포함한 다양한 기기에서 악성코드의 실행과 전파를 막을 수 있는 솔루션이 될 것이다.

주제어 : 스마트 단말 보안, 가상화, 도메인 분리, 안전실행환경(TEE), 신뢰 군사 영역(TMZ), 스마트워크

* 이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(R0101-16-0195, 모바일 단말의 비인가 접근 차단 및 안전한 운영환경 보장을 위한 EAL 4급 군사용 융합 보안 솔루션 개발)

Received 17 October 2016, Revised 21 November 2016
Accepted 20 December 2016, Published 28 December 2016
Corresponding Author : Jeong Nyeo Kim
(Electronics and Telecommunications Research Institute)
Email: jnkim@etri.re.kr

ISSN: 1738-1916

1. Introduction

Due to dramatic supply increase of smart device, expansion of new mobile threats such as violation of privacy and mobile malignant code on mobile environment are expected. Especially, worm and viruses which are executed in mobile devices such as smartphone can cause performance decline of mobile device, illegal collection of personal information and virus infection towards other services. Therefore, it is important to prepare for that. Also, duplication and leak of store information in mobile device from theft/loss are claimed to be worried. Even open platform mobile device like android is targeted for hacking due to increased market preference on open platform for mobile devices. As above, there will be limitation with existing software based solution like anti-virus on response for expansion of service which is concentrated on open platform with enlargement of security threat. Application service level of security measures such as mobile vaccine and MDM can not prevent damages like leaking internal important information by being rooted.

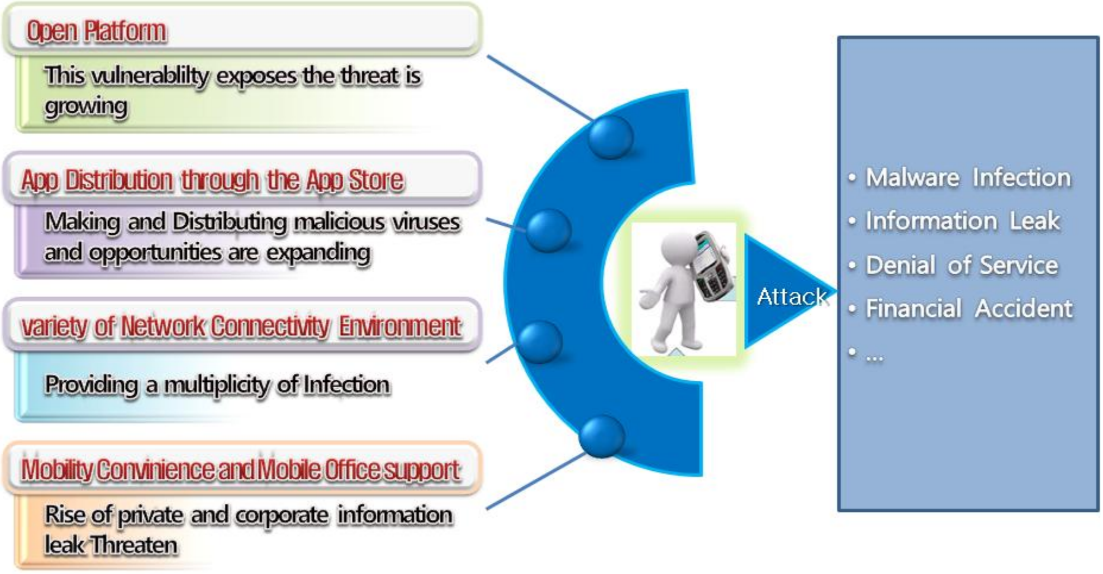
Especially, domestic smart device security technology consists of single-product technology at application level such as anti-virus, firewall, device lock function. It is possible to claim as relative beginning stage of technology. [1] TCG (Trusted Computing Group) announced MTM which is hardware security module for mobile environment. MTM is attached to mobile device to provide various security functions such as platform integrity valid function on device itself, shielding area, protection capability, safe key management system and physical safety. By that, it provides an environment that process and manage internal using file safely and valid integrity of device platform [3,4]. Development of a system level security platform technology is requested as top priority to protect open platform environment smart devices from aforementioned various security threats by considering characteristics of smart devices such as low-power, low-capacity, multimedia service and execution environment.

Due to dramatic advancement in performance and function of mobile devices, new various services based on mobile device are increased. In addition, dependency on mobile devices by users is getting increased. increasing number of new services provide convenience on our life, but those are also causing various security threats. Therefore, it is necessary to develop security platform that can be prepared for security threats and malicious attack [5]. TEE (Trusted Execution Environment) of Global Platform which means separated trusted execution environment from general mobile operating system (ex: Android OS) and applications is representative as security platform structure [6]. TEE provides an operation environment which is more safe than general operation system like android. Also, it provides methods to provide high security level with low cost even without attaching hardware based SE (Secure Elements). In TEE structure, application from general mobile operation system need to use defined API by TEE for using security services (password, safe save, etc.) of TEE. However, there is a possibility that malicious application can penetrate TEE area through TEE API.

This paper figures out implementation of virtualization based smart device security technology which provides platform level of security functions about smart devices and mobile security device structure which has isolated safe execution area based on TEE.

2. Smart Device Security Threaten

It is possible to divide security threats for smart devices. The first one is enlargement of exposure and security vulnerability due to open platform. Second is expanding spreads opportunity and creation of malicious viruses by distribution of application through app store. Third is providing diversity of infection path


Open Platform
This vulnerablilty exposes the threat is growing
App Distribution through the App Store
Making and Distributing malicious viruses and opportunities are expanding
variety of Network Connectivity Environment
Providing a multiplicity of Infection
Mobility Convinience and Mobile Office support
Rise of private and corporate information leak Threaten
Attack
• Malware Infection
• Information Leak
• Denial of Service
• Financial Accident
• ...

[Fig. 1] Smart Device Security Threaten

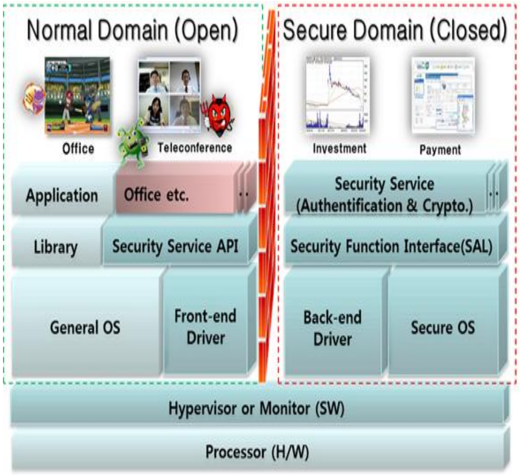
by supporting variety of network connection. Final one is enlargement of company and personal information exposure due to portability and mobile office support.

Also damages also continue as infection of malicious code, exposure of company/personal information, denial of service attack and financial accidents.

By looking mobile malicious code infection path ratio of the world, Bluetooth 67.1%, MMS (24.4%), external storage device (3.7%), PC plug-in (2.4%) and Internet download (2.4%). To protect smart devices from those various security threats, platform security technology is required.

3. Security Technology Implementation of TEE-based smart device

This paper designed a mobile security platform with TEE based safe execution area structure based on TeeMo which is developed as mobile security platform [7,8]. TeeMo has android area and safe execution area based on virtualization device. Application of android field uses services in safe execution area through owned defined security API. This paper suggests safe execution environment based on TEE that can protect important information in mobile devices as [Fig. 2]. This mobile safe execution area can provide various security functions based on TEE for application programs from mobile.



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

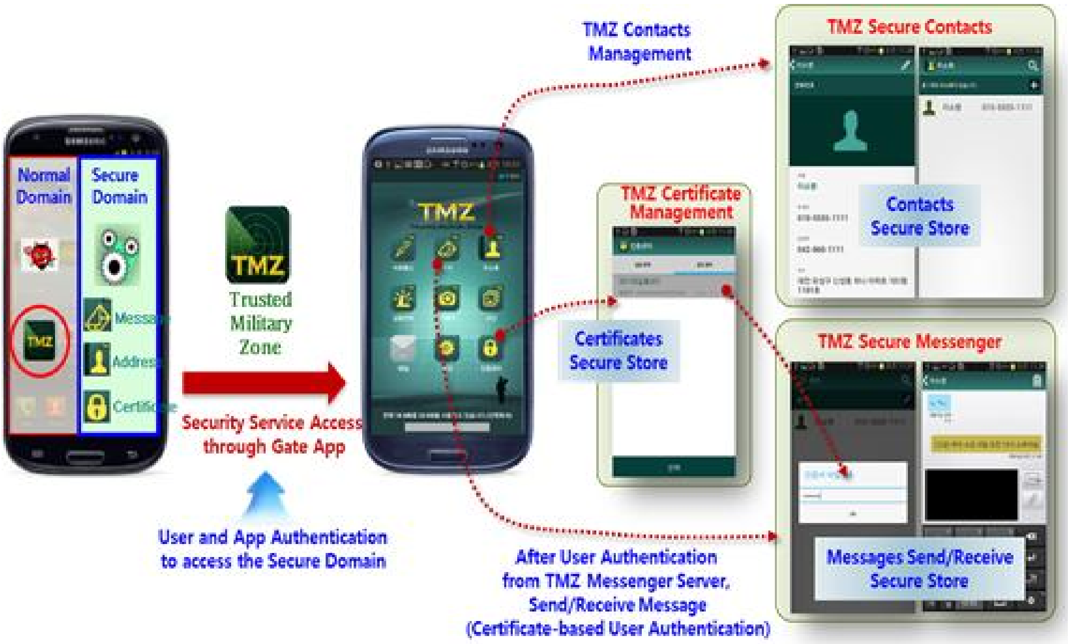
4. Implementation And Test Result

Most of mobile malicious code are infected by sending SMS message and email. Mobile malicious code is usually downloaded and installed in user's smart device by pretending as normal application. Attacker inputted malicious code on an app. When the malicious application is successfully installed and executed, malicious code will collect sensitive data in smart devices like SMS messages, contacts, photos and certificates. Especially, certificate is the most important and sensitive data that is widely used for mobile banking and payment in Korea. This technology detects and prevents information leak from smart devices even it is infected by mobile malicious code. All security services are only executed and approached through TMZ(Trusted Military Zone) which is a gate application. Especially, it provides safe military text/status transmit application service through TMZ Text, TMZ Contacts, TMZ verification management. By that, it prevents exposer of information such as text, contact and certificate.

[Fig. 3] shows a prototype of domain separation based smart device security platform. This platform includes security engine and security API which include password software and hypervisor in commercial smartphone.

This section shows functional consideration of smart device security platform which uses hypervisor. This security platform guarantees that safety and trusty of mobile security services such as mobile office and mobile conference. For that, this paper suggests 4 components such as domain separation by Hypervisor, Secure OS, trusted channel and security API.

Even mobile malicious code is executed in general area of smart device and try to steal information in smart device, it is impossible since all confidential military information is saved in safe domain. For mobile vaccine, it can't detect change of permitted


TMZ Contacts Management
TMZ Secure Contacts
Normal Domain
Secure Domain
TMZ
Messa
Addres
Certifica
TMZ
Trusted Military Zone
Security Service Access through Gate App
User and App Authentication to access the Secure Domain
TMZ
TMZ Certificate Management
Certificates Secure Store
Contacts Secure Store
TMZ Secure Messenger
Messages Send/Receive Secure Store
After User Authentication from TMZ Messenger Server, Send/Receive Message (Certificate-based User Authentication)

[Fig. 3] Domain Separation-based Smart Device's security platform prototype system library since it is security solution based on software. Also, mobile vaccine can not detect a new mobile malicious code if malicious code pattern is not existed in DB. By that it is possible to overcome limitation of mobile vaccine through this technology.

5. Conclusion

This paper figures out domain separation based device security platform technologies which are necessary for smart devices. Meanwhile, domain separation based smart device security platform from this paper can provide various security functions which are necessary for application program in mobile devices rather than existing hardware based security technology which only provides source of trust function on mobile device. The domain separation based smart device security platform technology blocks unauthorized access and leakage of sensitive information in device. Also it will be the solution can block transmission and execution of malicious code in various area including variety of IoT devices in internet rather than just smart devices. Due to introduction of various and new IoT services, increase of communication and connection among numerous devices has various specification and characteristic is expected. Due to characteristics of those IoT service environment, there must be a lot of security threats. To respond on that, development of safe service environment and reinforcement of service security must be involved. After, a research will be planned to conducted to find a method to secure trusty and security by using IoT devices that can synchronize with security hardware, gateway security technology and hypervisor which is domain separation technology on various IoT devices.

ACKNOWLEDGEMENT

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (R0101-16-0195, Development of EAL 4 level military fusion security solution for protecting against unauthorized accesses and ensuring a trusted execution environment in mobile 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] Bickford J., O'Hare R, Baliga A, Ganapathy V, and Iftode L, "Rootkits on Smart Phones: Attacks, Implications and Opportunities," in Workshop on Mobile Computing Sys. and Appl. (HotMobile'10). ACM, Feb. 2010.

[6] Global Platform Device Technology, "The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market," Global Platform WhitePaper, Feb. 2011.

[7] Kim Y.-H, Lee Y.-G, Kim J.-N, "TeeMo: A Generic Trusted Execution Framework for Mobile Devices," International Conference on Computer, Networks, Systems, and Industrial Applications (CNSI), pp.579-583, July 2012.

[8] Kim Y.-H, Kim J.-N. "Building Secure Execution Environment for Mobile Platform," First ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering, pp.119-122, 2011

[9] Onechul Na, Hyojik Lee, Soyoung Sung, Hangbae Chang, "A Study on Construction of Optimal Wireless

Sensor System for Enhancing Organization Security Level on Industry Convergence Environment", Journal of the Korea Convergence Society, Vol. 6, No. 4, pp. 139-146, 2015

[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