Security Core Technology Implementation for Hardware-based Smart Devices

JeongNyeo Kim and Yong-Sung Jeon
Mobile Security Research Section, Information Security Research Division
Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea

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.

Introduction
Expansion of new mobile threats 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 threats. 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.

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.

Figure1. Smart device security threaten
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.

**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 Figure2. This secure execution environment for mobile device can provide various MTM-based security functions for application programs in mobile device.

**Implementation and Test Result**

Most of the mobile malwares are infected by sending SMS messages or emails. 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 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.

**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 securitythreatens 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 research paper was funded by the Government (Ministry of Science, ICT and Future Planning) and sponsored by IITP. (No. R-20150518 - 001267001267001267001267001267001 267, Title: Operating System Security Core Technology Development for Smart Lightweight IoT)

**References**


