Trusted Mobile Zone: A Mobile Hypervisor Based Security Platform for Reliable Mobile Service

Kyung-Soo Lim*, Jae-Deok Lim, and Jeong-Nye Kim
EIectronics and Telecommunication Research Institute, Daejeon, Republic of Korea
{lukelim, jdscol92, jnkim}@etri.re.kr

Abstract

As smart devices expand to our lives rapidly, its popularity has become the attractive targets for malicious attackers. For the countermeasures of security threats, the techniques of trusted execution environment with domain isolation have emerged to enhance reliability and confidentiality for preserving sensitive information. This paper describes a mobile hypervisor based security platform supporting various mobile services. Our suggested platform based on hypervisor-based domain isolation is able to protect sensitive information against unauthorized accesses and provide a trusted execution environment with reliable data processing and identity authentication. We also present a prototype solution to show how our platform applies into mobile services.

Keywords: Mobile Security, Security Platform, Domain Separation, Mobile Hypervisor

1 Introduction

The smart devices with easy Internet accessibility, mobility and usability are various service environment such as mobile office, smart work, mobile finance, e-government and so on.[7] On the other hand, security threats to these devices have been also increased by malicious attacks such as malware, ransomware, and smishing. Especially, due to the openness of the Android app market, the distribution of malicious applications developed by attackers is increasing rapidly.

Meanwhile, the architecture of Android app can be easily reversed and repacked. For example, the attacker downloads the particular normal app from Android open market and unpacks its app package file (apk). Next, he or she inserts malicious codes in normal app after decompiling binary data. Finally, he creates malicious app in the reverse order of previous steps and upload it to Android app market for inducting common user. Most of malicious apps can access and view sensitive information in the infected devices. The extortion of the private information due to those attacks can be damaged the integrity and reliability. Thus, mobile services on the smart devices need to improve reliability against malicious attacks, such as providing trusted execution environments, handling sensitive information securely and protecting the business or finance applications.

Likewise, the security technology is an essential part of operating mobile services on smart device. It is necessary with considering private credentials protection or preventing data leakages as a security countermeasure. Nowadays, the domain separation technology has emerged for Android devices. It separates an ordinary smart device environment to diverse domains, such as normal and secure domain. The normal domain is almost identical existing smart device environment such as Android OS.[1][5] On the other hand, the isolated secure domain with the secure OS environment protects user's sensitive information and performs trusted execution, such as finance transaction, business application, and military service, respectively.

IT CoNvergence PRActice (INPRA), volume: 4, number: 3 (September 2016), pp. 28-34

*Corresponding author: Information Security Research Division, EIectronics and Telecommunication Research Institute, 218 Gajeong-ro, Yuseong-gu, Daejeon, Republic of Korea, Tel: +82-42-860-5952

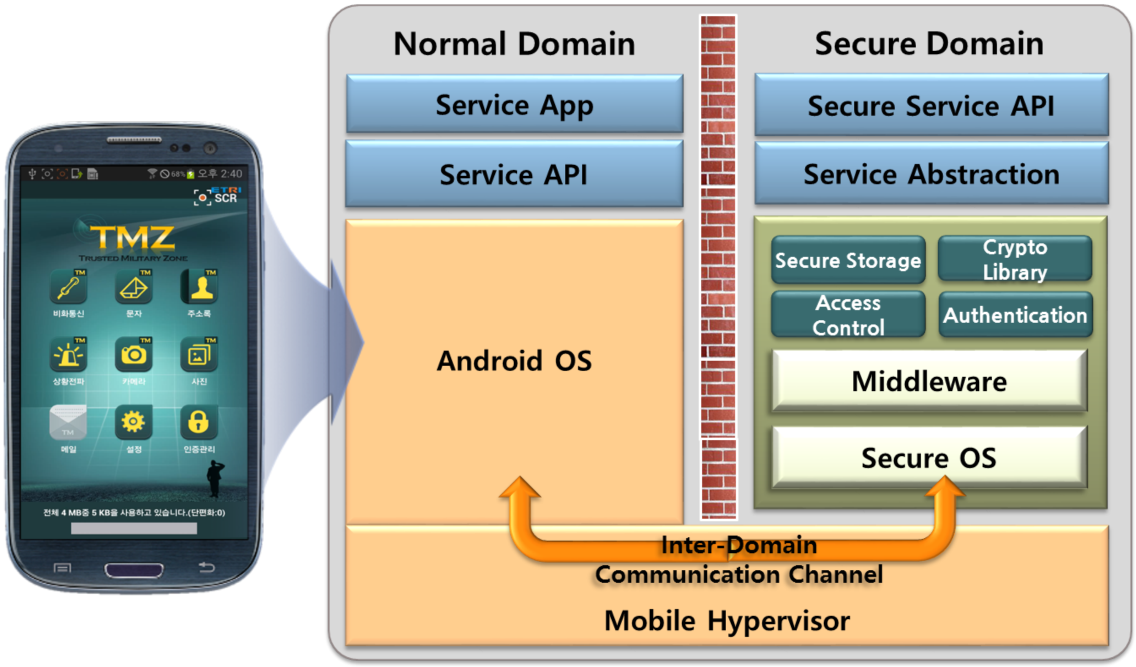

Figure 1: Structure of mobile hypervisor based security platform

In this paper, we suggest a mobile hypervisor based security platform supporting diverse mobile services. Our suggested platform, we called Trusted Mobile Zone (hereinafter TMZ), has been developing in order to ensure essential security applications for widely used smart devices using two divergent domains isolated by the mobile hypervisor.[5] Our platform based on secure domain can protect sensitive information against unauthorized accesses and ensuring a trusted execution environment for reliable data processing and identity authentication management. And we will have plans to deploy our platform to various mobile-based services such as, smart work, military service, e-government, and secure BYOD (Bring Your Own Device) service.

2 Trusted Mobile Zone: Mobile Hypervisor based Security Platform

This paper presents a mobile hypervisor based security platform supporting mobile service. TMZ platform has been developing in order to ensure essential security applications for widely used smart devices, using two divergent domains with separated execution environment, as secure domain for operating security service with a trusted execution environment versus normal domain for existing mobile operating system such as Android OS. Our platform can protect sensitive information against unauthorized accesses and ensure a trusted execution environment for reliable data processing. TMZ platform provides more enhanced secure functions compare with general smart devices. As earlier research [7], we described functional considerations for military-grade mobile security platform and suggest these as requirements for mobile secure platform. We has been researching and developing TMZ platform with extending the previous research. The followings are main features of TMZ platform.

- Domain Separation
- Secure File management
- Secure Middleware

- Access Control
- Cryptography Library
- Authentication management
- Secure Service API

First of all, the mobile hypervisor based domain separation is an essential part of security platform to protect sensitive information against unauthorized or illegal accesses. The domain separation with mobile hypervisor is able to provide the trusted execution environment for identity authentication and sensitive data processing. [2] Although security enhanced Android platform [3] are adopted in recent secure measures, the domain separation using hypervisor is more secure than Android OS itself, because it is able to operate different OS environment and consolidate security features in the isolated domain. [5]

TMZ provides secure filesystem and management feature. The secure file management is important to protect confidential or sensitive information in case of stolen or lost the device situation. The secure file management can be consist of secure filesystem with file encryption, secure deletion for protecting file recovery, continuously file defragmentation on the particular maintenance period, etc. Moreover, secure filesystem is located and operated on the volatile memory of the smart device using the characteristic of type 2 hypervisor. It means when the device is powered-off, the filesystem is wiped and unable to recover user data. Naturally, TMZ also provides the dumping/loading feature of filesystem image when it prepared for rebooting. The filesystem images are saved the storage device of Android platform, however this image file are encrypted by cryptography algorithm such as AES 128bit.

Secure Middleware offered by TMZ can protect inter-domain channel [4] against malicious attacks such as man-in-the-middle-attack into the domain channel. The encrypted inter-domain channel will be more reliable than encoded message communications. On the other hand, it can have a side effect as performance reduction, but it supports an appropriate level of performance reduction as much as a common user can tolerate. We will describe the performance issues on the following chapter. Most of the file size of single photo will not be exceeded almost 1 Megabytes in ordinary smart devices. Thus, TMZ provides large message transportation on the inter-domain channel either [7].

The access control feature is a fundamental feature in TMZ to protect unauthorized access. It supports two-factor authentications by a user and an application who/which request security services in the secure domain. Moreover, TMZ checks and verifies the integrity of TMZ applications periodically as an essential part of access control features. The authentication management in TMZ is complied with FIPS-196 standard to provide mutual authentications with remote servers for user or device confirmations. This feature supports electronic authentications based on KCDSA (Korean Certificate-based Digital Signature Algorithm) and RSA digital signature. The cryptography library is composed of symmetric key, public key, hash algorithm, and authentication library. It is a core part of operating each modules of TMZ platform such as file encryption, digital signature for certificates and others. Finally secure service API provides APIs for developing secure functions of TMZ app implementation.

3 Use Case: TMZ based Mobile Services

TMZ is a prototype solution of the ongoing research project to develop military-grade security mobile solution based on security platform with mobile hypervisor. The final goal of our project is to acquire the CC EAL4 certification for TMZ platform. As shown as figure 2, the prototype app services of TMZ provides military security service including secure SMS and MMS, contacts, camera, gallery, secure voice communication, and emergency situation notice. These app services are operated in Android OS

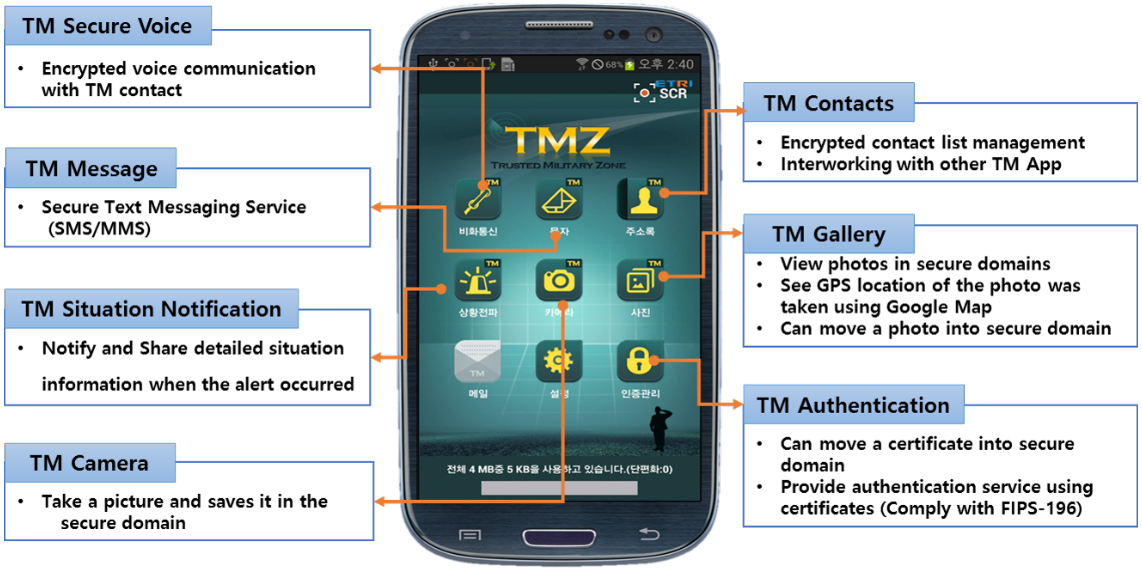
TM Secure Voice
• Encrypted voice communication with TM contact
TM Message
• Secure Text Messaging Service (SMS/MMS)
TM Situation Notification
• Notify and Share detailed situation information when the alert occurred
TM Camera
• Take a picture and saves it in the secure domain
TM Contacts
• Encrypted contact list management
• Interworking with other TM App
TM Gallery
• View photos in secure domains
• See GPS location of the photo was taken using Google Map
• Can move a photo into secure domain
TM Authentication
• Can move a certificate into secure domain
• Provide authentication service using certificates (Comply with FIPS-196)
오후 2:40
ETRI SCR
TMZ
TRUSTED MILITARY ZONE
TM
비화통신
문자
주소록
상황전파
카메라
사진
메일
설정
인증관리
전체 4 MB중 5 KB을 사용하고 있습니다.(단편화:0)

Figure 2: Mobile Services based on TMZ platform

environment, however, all the data was shown in these apps are transferred from the secure domain when it needs to view by the user actions. TMZ platform and service apps has been installed and tested to a commercial smart device, as Samsung Galaxy S3 LTE. Currently, we have been testing on a novel device such as Google Nexus 6P.

The mobile services based on TMZ are similar to essential features of the ordinary smart phone. TMZ provides text messaging service including SMS and MMS, contacts list, camera, photo gallery, secure voice communication, and emergency situation notice app. These services were developed based on the requirements of the advisory committee consisting of Korean military officials. The following figure 3 shows examples of TMZ mobile applications.

TM contacts are the exclusive address book app for TMZ environment. It encrypts contact lists on secure filesystem and it takes a part of main role for interworking with other services such as text messaging, secure voice communication, etc. TM messages are similar to general messaging app with sending and receiving messages. It operated and connected with special-purpose messaging server for TMZ environment. TM secure voice app provides encrypted voice communications with other TMZ users, which is operated on SIP (Session Initiation Protocol) with TURN (Traversal Using Relay NAT) server. TM camera and gallery provides the same functionality comparted to the existing smart phone except for data encryption and isolation. And TM gallery retrieves the GPS location of the picture taken using Google map. Also TMZ user can move photo images of normal domain to secure domain using TM gallery app. TM authentication service provides digital signature functions based certificates for user authentication. It also manages and verify user certificates through the authentication server. TM situation notice has come close to the military-purpose service compared with other TM apps. In the focus of application level, the operating mechanism is similar with TM message. On the other hand, the control server for situation monitoring provides viewing and managing the emergency situation when an alert occurs in a field. When the emergency or alert occurred by a sentry in the field operation, he takes a photo and write a message for detailed description. Next, he sends MMS to the control server in the military office. The watch control server receive this message and retrieve GPS location of this alert, finally it spreads it to a chief officer and nearby sentries to response further actions.

The following table is file acquisition time according to the file types such as text messages, contact list and photo images. This experiment result is described the previous research paper [6], which is pre-

Table 1: File Acquisition Experiment through Secure Domain

File Acquisition Time		
File Type	File Size (bytes)	Avg Time (sec)
Text Messages	3,504	0.031
Contact Lists	520	0.017
Image Files	654,532	1.602

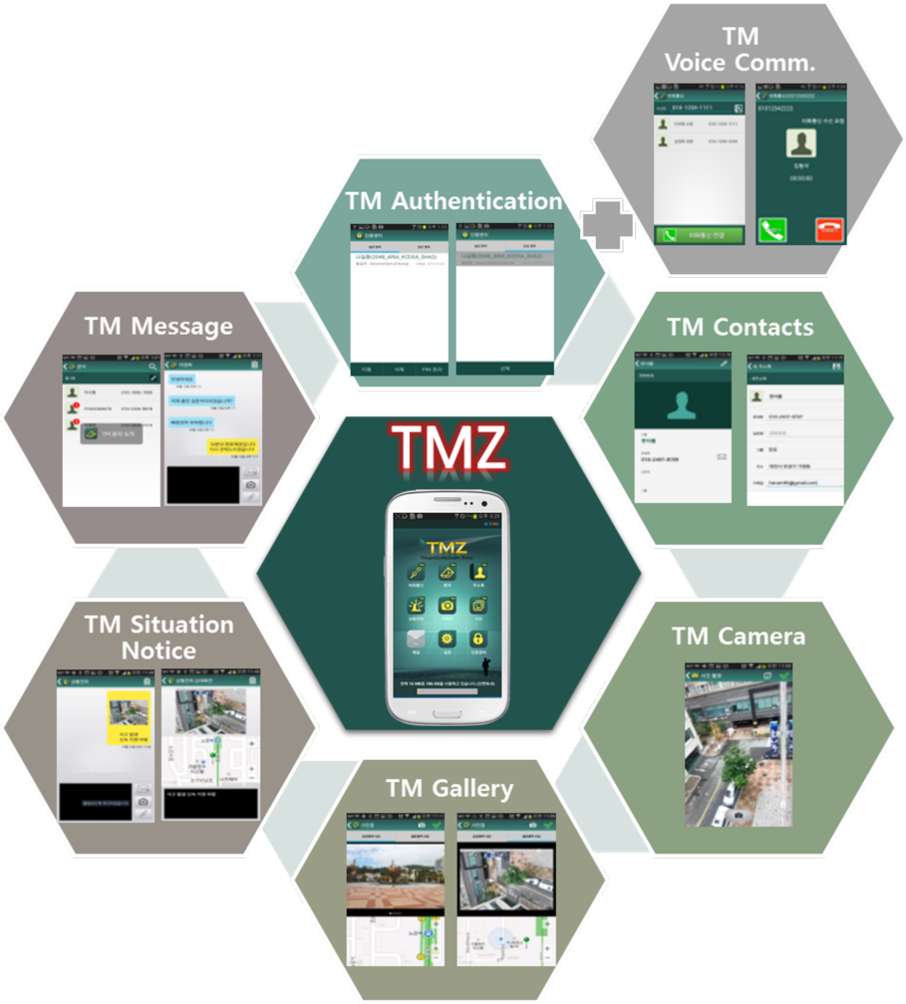

Figure 3: Examples of TMZ Mobile Applications

sented on the international conference. The file acquisition time includes total time for data acquisition based on mobile hypervisor with inter-domain communication. As the result of table 1, the most of file acquisition time are less than 0.05 seconds except for photo image. If we reduce the quality of photo image file, the estimated time for acquisition will be able to reduce on the suitable level timely. Moreover, the average signing time for KCDSA certificates according to unilateral authentication takes 2.109 second, moreover, in case of mutual authentication takes 4.952 second. It shows that TMZ have a side effect as performance reduction because of mobile hypervisor, but it provides the appropriate level of performance as a typical user can tolerate.

4 Conclusion and Future works

In this paper, we suggest a mobile hypervisor based security platform supporting mobile service. Our suggested platform, we called Trusted Mobile Zone (hereinafter TMZ), has been developing in order to ensure essential security applications for widely used smart devices, using two divergent domains with separated execution environment, as secure domain for operating security service with a trusted execution environment versus normal domain for existing mobile operating system such as Android OS. Our platform can protect sensitive information against unauthorized accesses and ensuring a trusted execution environment for reliable data processing and identity authentication. TMZ is a prototype solution of the ongoing research project to develop military-grade security mobile solution based on security platform with mobile hypervisor. The prototype app services of TMZ provides military security service including secure SMS and MMS, contacts, camera, gallery, secure voice communication, and emergency situation notice. These app services are operated in Android OS environment, however, all the data was shown in these apps are transferred from the secure domain when it needs to view by the user actions.

As we described, TMZ supports various security enhancement, on the other hand, performance reduction is an inevitable issue compared with general smart device. However, TMZ supports an appropriate level of performance that a typical user can tolerate. Thus, we are currently researching to improve performance of TMZ platform for the future works. And we will try to deploy our products to various mobile-based services to provide security such as, military service, secure smart work, e-government, and secure BYOD (Bring Your Own Device) service.

Acknowledgments

This work was supported by Institute for Information and 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] J. Andrus, C. Dall, A. V. Hof, O. Laadan, and J. Nieh. Cells: a virtual mobile smartphone architecture. In *Proc. of the 23rd ACM Symposium on Operating Systems Principles (SOSP'11), Cascais, Portugal*, pages 173–187. ACM Press, October 2011.

[2] P. Colp, M. Nanavati, J. Zhu, W. Aiello, G. Coker, T. Deegan, P. Loscocco, and A. Warfield. Breaking up is hard to do : Security and functionality in a commodity hypervisor. In *Proc. of the 23rd ACM Symposium on Operating Systems Principles (SOSP'11), Cascais, Portugal*, pages 189–202. ACM Press, October 2011.

[3] T. Frenzel, A. Lackorzynski, A. Warg, and H. Hartig. Arm trustzone as a virtualization technique in embedded system. In *Proc. of the 12th Real-Time Linux Workshop (RTLWS'10), Nairobi, Kenya*, pages 1–1, October 2010.

[4] K. Kim, C. Kim, S.-I. Jung, H.-S. Shin, and J.-S. Kim. Inter-domain socket communications supporting high performance and full binary compatibility on xen. In *Proc. of the 4th ACM SIGPLAN/SIGOPS international conference on Virtual execution environments (VEE'08), Seattle, Washington, USA*, pages 11–20. ACM Press, March 2008.

[5] Y.-H. Kim, Y.-K. Lee, and J.-N. Kim. Teemo: A generic trusted execution framework for mobile devices. In *Proc. of the International Conference on Computer, Networks, Systems, and Industrial Applications (CNSI'12), Jeju Island, Korea*, pages 579–583, July 2012.

[6] Kyung-Soo, Y. sung Jeon, J.-N. Kim, and D.-G. Lee. A methodology for live forensic acquisition in secure domain based on domain separation technology. In *Proc. of the 2nd International Conference on Communication and Computer Engineering (ICOCOE'15), Phuket, Thailand, LNCS*, volume 362, pages 1113–1123. Springer-Verlag, June 2015.

[7] K.-S. Lim, S.-W. Park, J.-N. Kim, and D.-G. Lee. Functional considerations in military-grade security platform using a mobile hypervisor. *Computer Science and its Applications*, 330:1413–1418, 2015.

Author Biography

Kyung-Soo Lim receivecd M.S. degree and Ph.D. in Graduate School of Information Management and Security from Korea University, Rep. of Korea, in 2008 and 2013, respectively. He is currently a senior researcher of Information Security research division in Electronics and Telecommunications Research Institute (ETRI) since 2010. In addition, He has also served as chairs and members of program committees for many international conferences and workshops. He has been serving as a guest editor for international journals by some publishers. His research interests include information security, digital forensics, mobile security, intelligent video surveillance etc.

Jae-Deok Lim JaeDeok Lim received his M.S. degree in Electronic Engineering from Kyungbook National University, Rep. of Korea, in 2001 and the Ph.D in Computer Engineering from Chungnam National University, Korea, in 2013. He is currently a principal researcher at Cyber Security Research Division in Electronics and Telecommunications Research Institute (ETRI). His research interests include IoT security, mobile security, secure operating system, access control and system security.

Jeong-Nye Kim received her M.S. degree and Ph.D. in Computer Engineering from Chungnam National University, Rep. of Korea, in 2000 and 2004, respectively. She studied at computer science from the University of California, Irvine, USA in 2005. Since 1988, she has been a principal member of engineering staff in Electronics and Telecommunications Research Institute (ETRI), where she was worked as a Managing Director of the Cyber Security System Research Department until 2016. Her research interests include IoT security, mobile security, secure operating system, network security and system security.