Trusted Mobile Zone Solution Based on Virtualization Technology

GeonLyang Kim, JeongNyeo Kim
Information Security Research Division
Electronics and Telecommunications Research Institute
Daejeon, Republic of Korea
e-mail: glkim@etri.re.kr, jnkim@etri.re.kr

***Abstract*—We developed a Trusted Mobile Zone (TMZ) solution based on virtualization technology for smart mobile devices. This solution offers users a trusted execution area to preserve significant files, and execute security services in a secure manner. In addition, it is able to block attackers from leaking significant files. We simulated a Smishing attack to obtain significant data from a Secure Zone (SZ) of the TMZ solution, the results of which are described herein.**

Keywords-BYOD; Mobile Security; TEE; Virtualization.

I. INTRODUCTION

As the use of mobile devices rapidly increases, personal smart mobile devices are being used for business purposes. Solutions for blocking the outflow of enterprise files, such as Knox [1] and Cellrox [2], are urgently needed. We developed the Trusted Mobile Zone (TMZ) solution to offer better data leakage prevention services to users. Unlike Knox and Cellrox, the security functions of the TMZ solution operate on a secure OS different from a normal OS, and the proposed solution therefore has the advantage of being less vulnerable to malicious codes or attacks aiming at obtaining significant files by exploiting the vulnerabilities of a normal OS. The TMZ solution was designed with reference to the Global Platform's Trusted Execution Environment (TEE) system [3]. It offers a trusted execution area to preserve significant files and provide trusted services securely through secure components.

II. TMZ SOLUTION ARCHITECTURE

The TMZ solution supplies a higher level of security without paying additional costs through the addition of hardware [4]. The hypervisor as a virtualization technology has two types: a type 1 hypervisor as a native or bare-metal hypervisor, and a type 2 hypervisor as a hosted hypervisor [5]. A type 1 hypervisor offers a higher level of security than a type 2 hypervisor.

The TMZ solution can be built on a mobile device regardless of the hypervisor type applied. KNOX runs on Android OS, and provides kernel-level access control through SE Android. Most products including Horizon Mobile of VMWare offer the only separation of an Open OS and a Secure OS. However, the TMZ solution separates the General Zone (GZ) and SZ using a hypervisor. It also provides trusted security services for users through the use of security components including the SZ. The security components of the TMZ solution provide users with functions to store significant data, create signature data, deposit encryption and decryption keys, and preserve private keys for signature data, all in a secure manner. It also offers an encrypted communication channel for transmitting significant data securely between a GZ and an SZ. The architecture of the TMZ solution is shown in Figure 1.

The only GZ-Security API in a GZ is able to access an SZ through an encrypted communication channel. We defined the GZ-Security API of five groups and developed security applications that can offer trusted security services using an SZ through the GZ-Security API.

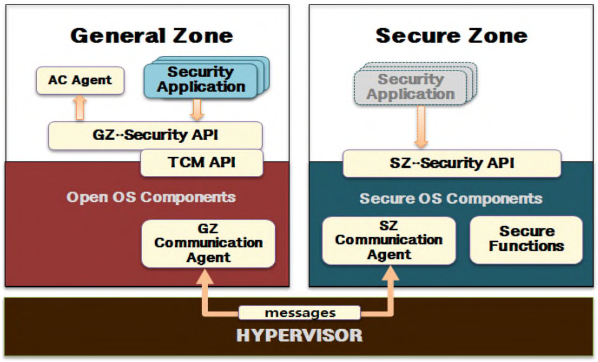
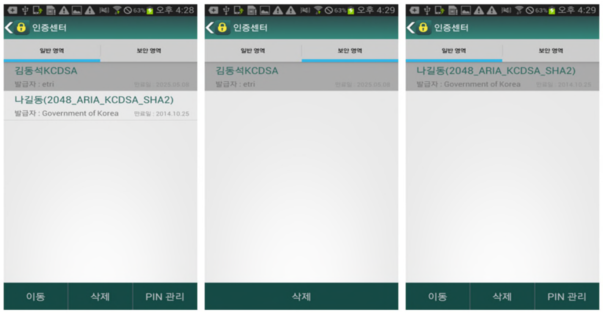


Figure 1. TMZ solution architecture

III. DATA LEAKAGE PREVENTION SERVICES USING THE TMZ SOLUTION

We implemented data leakage prevention services, including a Trusted Certificate Store Service, Trusted Contact Service, Trusted Camera Service, and Trusted Gallery Service, using the TMZ solution. When hacking tools are used, general files in a GZ are spilled out, whereas significant files managed in an SZ are not spilled into a GZ or to the outside.



김동석KCDSA
발급자 : etri 만료일 : 2025.05.08
나길동(2048_ARIA_KCDSA_SHA2)
발급자 : Government of Korea 만료일 : 2014.10.25

김동석KCDSA
발급자 : etri 만료일 : 2025.05.08

나길동(2048_ARIA_KCDSA_SHA2)
발급자 : Government of Korea 만료일 : 2014.10.25

Figure 2. Screen shots of Trusted Certificate Service

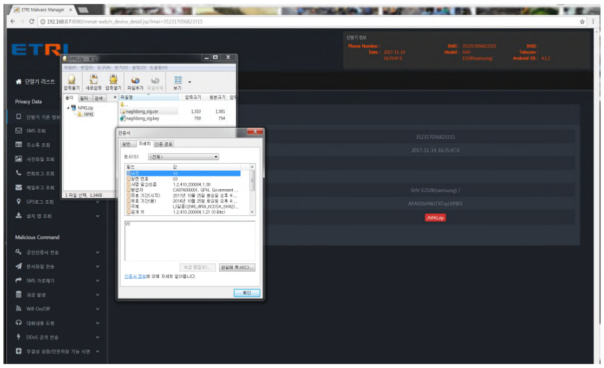
ISBN: 978-1-61208-622-4

Certificate files, including the private key file, are saved and managed in general storage that attackers are able to easily enter or release to the outside. Therefore, they are threatened by leaks and misuse by malicious users. If they are leaked to the outside, their owners can suffer damage through illegal authentication.

With a Trusted Certificate Service, the certificate files in a GZ are saved and managed in an SZ of the TMZ solution. This blocks the outflow of significant files for illegal authentication. The files are securely encrypted and managed in the SZ. Significant files, such as encryption key files, sensitive image files, and important contact files cannot be spilled out of the SZ into a GZ, and are secure.

IV. Smishing Attack Simulation on TMZ Solution

We proposed the TMZ solution for blocking the illegal outflow of significant files. The TMZ solution supplies a trusted execution area isolated from the GZ, where a large number of threats can occur and many vulnerabilities exist. The SZ operates on a different secure OS through Android OS of the NZ. This is more secure because the weaknesses of Android OS are not applicable to a secure OS. Therefore, the TMZ solution supplies trusted security services to users.



단말기 정보
Phone Number :
Date : 2017-11-14 16:35:47.0
IMEI : 352317056823315
Model : SHV-E210K(samsung)
IMSI :
Telecom :
Android OS : 4.1.2

파일명	압축크기	원본크기
nagildong_sig.cer	1,310	1,381
nagildong_sig.key	759	754

1 파일 선택, 1.34KB

필드	값
버전	V3
일련 번호	03
서명 알고리즘	1.2.410.200004.1.38
발급자	CA974000001, GPKI, Government ...
유효 기간(시작)	2011년 10월 25일 화요일 오후 4:...
유효 기간(끝)	2014년 10월 25일 토요일 오후 4:...
주체	나길동(2048_ARIA_KCDSA_SHA2)...
공개 키	1.2.410.200004.1.21 (0 Bits)

V3

인증서 정보에 대해 자세히 알아봅니다.

352317056823315
2017-11-14 16:35:47.0
SHV-E210K(samsung) /
APA91bHWzTXTxyUtPBf3

Figure 3. Files spilled out of GZ and into a hacking server

We simulated a Smishing attack to obtain significant data from an SZ of the TMZ solution. When a user applying the TMZ solution receives a Short Message Service (SMS) message and connects to a URL link in the message, a hacking application is installed and run.

After the hacking application is installed and executed through the message used in the Smishing attack, the general files in the GZ of the TMZ solution are transmitted to the hacking server. The user using the TMZ solution should manage their significant files in an SZ to block their outflow, including certificate files, contact files, and important image files.

Figure 3 shows files leaked from the hacking application of the GZ to the hacking server. The files transmitted from the TMZ solution to the hacking server through the hacking application are general files in the GZ of the TMZ solution. Figure 2 shows the certificate files in the GZ and SZ of the TMZ solution. We are able to know that the files spilled out from the TMZ solution and into the hacking server were the certificate files stored in the GZ of the TMZ solution.

V. Experiment Results

We calculated the time required to insert the certificate files securely from a GZ to an SZ. We built ETRI's VIMO type 2 hypervisor on Galaxy S3, and built μC/OS-II as a secure OS in the SZ for the TMZ solution. We calculated the required time 20 times in both the SZ and the GZ, the results of which are shown in Figure 4.

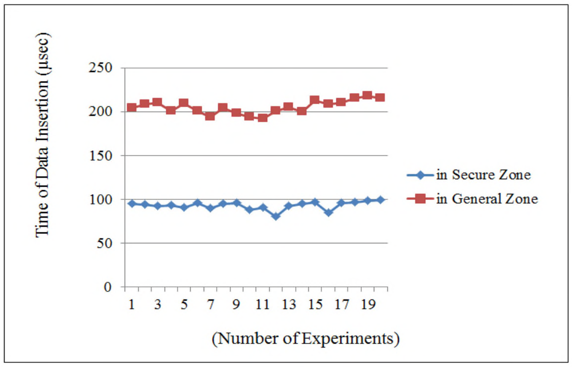


Figure 4. Performance measurement results

The calculated average value of insertion of certificate files in the GZ is 205 μsec, and in the SZ is 93 μsec.

VI. Conclusion

In this paper, we proposed a TMZ solution for blocking the illegal outflow of significant files. We simulated a Smishing attack to obtain significant files from the TMZ solution, and the files of SZ in the TMZ solution are not leaked. The TMZ solution can supply several security services by blocking the outflow of significant files in an SZ isolated from a GZ.

Acknowledgment

This work was supported by an Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) [No. 2015-0-00508, Development of Operating System Security Core Technology for the Smart Lightweight IoT Devices].

References

[1] https://www.samsungknox.com/docs/SamsungKnoxSecuritySolution.pdf, Samsung Knox White Paper: Samsung KNOX Security Solution Version 2.2, May 2017.

[2] Cellrox Homepage, http://cellrox.com, March 2018.

[3] https://www.globalplatform.org/specificationsdevice.asp, "TEE System Architecture v1.1," Global Platform, January 2017.

[4] D. Jaramillo, B. Furht, and A. Agarwal, "Virtualization Techniques for Mobile Systems," Multimedia Systems and Applications, Springer International Publishing, 2014.

[5] G. J. Popek, R. P. Goldberg, "Formal Requirements for Virtualizable Third Generation Architectures," Communications of the ACM, 17(7):412-421, 1974.