Proceedings of 2013 International Symposium on Embedded Technology(Interactive Session Only)
(ISET 2013)
Daegu Metropolitan City, 23-24 May, 2013.

Building the Android platform security mechanism using TrustZone

HeeJae Bae[*] Se-Won Kim[†] Chuck Yoo[†]

[*]Graduate School of Convergence IT
Korea University, Seoul, Republic of Korea
E-mail: beheebe@korea.ac.kr

[†]Collage of Information and Communication
Korea University, Seoul, Republic of Korea
E-mail: {swkim, chuckyoo}@os.korea.ac.kr

Abstract

Android has been extended gradually from mobile to other IT fields. But, Android which pursues an open environment has become a main target of the attackers and malicious codes have rapidly increased. The problem is that it is difficult for users to recognize malicious applications. In this paper, to solve this problem, TrustZone developed by ARM is used in the Android platform structure which provides system security mechanisms by separating Android into a Secure World and a Normal World.

Keywords: Android, TrustZone, Normal World, Secure World

1. Introduction

Malware[1] has been increasing explosively with the success of the smartphone market using Android platform. The malware is distributed free of charge into the Android smartphone in attempt to extort money through micro-payment systems and advertisements. However, these illegal behaviors of malwares are considered to be legitimate operations in the Android platform. The problem is that users unwillingly and without awareness permit the malware to be installed into their Android smartphone. In this paper, we present a secure Android system via TrustZone. It was designed to provide Android security mechanisms by SoC(System on Chip)level.

2. Security environment of Android platform using the TrustZone

When a user downloads and installs an application, the user would not know about the detailed operations. For example, specific application operations such as, where the contact numbers are used or where the message is being sent is difficult to be known by the user.[2] Also the user usually just agrees on frequent access permissions without even checking the contents. Malicious codes which exploit user's carelessness of security can execute other applications maliciously such as address book or SMS and extort important from them. (Figure 1)

TrustZone[3] is possible to store sensitive data in a safe location in order to protect it against access threats from the attackers and is a technique to enhance the security by the hardware. When a secure technology is applied to the hardware layer, the level of security at the next stage becomes more reliable. TrustZone supports the security of hardware and software components which consists of integrated ARM processor, and bus fabric.

We provide a virtualized structure, which separates process into a Normal World and a Secure World for running normal applications and secure applications respectively, by using TrustZone in Android.[4] The security bit through is divided into two separate Worlds by distinguishing. When the currently running virtual process is changed, it can be called using a monitor. By distinguishing the operations of the Normal World and the Secure World, the application of the Secure World can be protected from malicious codes in the Normal World during data communication. (Figure 2)

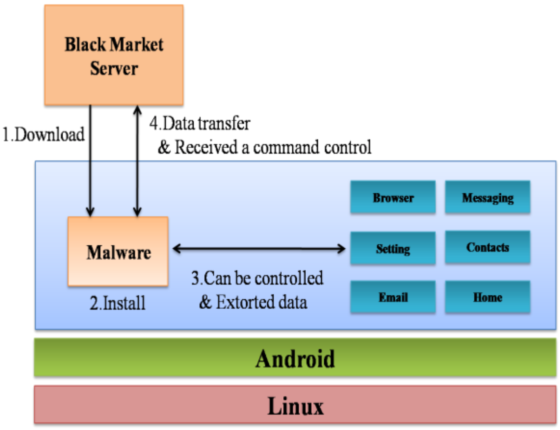

Figure.1

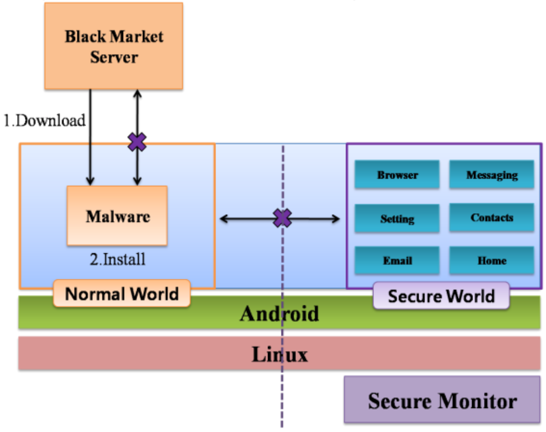

Figure.2

3. Conclusions

The main objective of the proposed model is to prevent the malware from careless user. If the application permissions are set in favour of the attackers, unintended malicious user operations are possible. This permission can be set in the manifest file, and should be utilized properly. Users just simply download and use the application, however, it is difficult for users possible to determine how the application to works. Therefore the manifest rights policy that was proposed in Android is not a sufficient security measurement.[5]

Also, there is a risk that sensitive information can leak to unintended recipients. This is a flow problem of Intra / Inter components of Android. When calling an internally protected function, due to unclear destination settings, information can be leaked. Android supports both explicit and implicit calls, but in order to support abundant services, implicit calls are inevitable. During this time of implicit calls, the attacker can extort data. The structure model of the system, proposed in this paper is to operate Android with separated a Normal World and a Secure World. As a result, applications and data which require safety can be protected without particular awareness from users.

Acknowledgement

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No.2010-0029180) with KREONET.

References

[1] Lookout, Lookout Mobile Threat Report, August 2011.
[2] A.P. Fuchs, A.Chaudhuri, and J.S.Fos- ter. Scandroid: Automated security certification of android. Technical Report UM Computer Science Department; CS-TR-4991, Department of Computer Science, University of Maryland, November 2009.
[3] ARM Limited, "ARM Security Technology: Building a Secure System using TrustZone Technology", http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.prd29-genc-009492c/index.html, 2009.
[4] S.Berger, R.Cáceres, K.A.Goldman, R.Perez, R.Sailer, and L.vanDoorn. VTPM: Virtualizing the trusted platform module. In Proceedings of 15th USENIX Security Symposium, Berkeley, CA, USA, 2006.
[5] W.Enck, M.Ongtang, and P.McDaniel. Understanding Android security. Security & Privacy, IEEE, 7(1):50–57, 2009.