Android Permission System Violation:
Case Study and Refinement

Kyoung Soo Han, Department of Computer and Software, Hanyang University, Seoul, South Korea

Yeoreum Lee, Department of Computer and Software, Hanyang University, Seoul, South Korea

Biao Jiang, Microsoft (China), Co., Ltd., Shanghai, China

Eul Gyu Im, Division of Computer Science and Engineering, Hanyang University, Seoul, South Korea

ABSTRACT

Android uses permissions for application security management. Android also allows inter-application communication (IAC), which enables cooperation between different applications to perform complex tasks by using some components and Intents. In other words, Android provides more flexibility and places less restriction on application development. This is a major feature that differentiates Android from its competitors. However, IAC also facilitates malicious applications that can collude in attacks of privilege escalation. In this paper, the authors demonstrate with case studies that all IAC channels can potentially be utilized for privilege escalation attacks, and the authors propose a refinement to solve this problem by enforcing IAC permissions and exposing IAC to users.

Keywords: Android Permission, Android Security, Permission-Based Security, Privilege Escalation Attacks, Smartphone Security

INTRODUCTION

Along with the rapid growth of the smartphone market and the expansion of the variety of smartphones available, the number of smartphone users is increasing rapidly. As a result, smartphones have already become an essential part of modern life because of convenience and extendibility through the various application installations. In addition, as they become increasingly powerful, they store more and more private user information, which makes them an attractive target for attackers.

Operation systems such as Android, iOS, Windows Phone, Symbian, and BlackBerry are necessary for the functionality of smartphones. Recently, Android operation system–based smartphones, which are composed of open

DOI: 10.4018/jeei.2013010102

platform systems, are attracting great attention from application developers. Android was announced by Google in 2007 (Open Handset Alliance, 2007) and became the most popular smartphone operating system by 2011 (Schonfeld, 2012). Compared with Apple's iOS and Microsoft's Windows Phone, Android provides more flexibility and places less restriction on application development. In particular, inter-application communication (IAC), empowered by inter-component communication (ICC), enables cooperation between different applications with different abilities to fulfill a task together even without knowing each other during development. IAC facilitates the achievement of complex goals, which may not be possible for operating systems without IAC. This is a major feature that differentiates Android from its competitors. However, IAC also weakens application-wise isolation and introduces the potential risk of privilege escalation. However, information can be leaked in various ways using this vulnerability, thus security technologies are required.

We have looked into this issue and found that every type of IAC available on Android is vulnerable to privilege escalation. In addition, we demonstrated this vulnerability using case studies on each IAC channel and provided details of subtle points that are usually ignored. Moreover, we obtained further insights into the current permission system on Android and proposed refinements.

This paper includes the following discussions: the importance of security in e-business, preliminary knowledge of Android, related work, attack model analysis, observation and refinement, conclusion, and directions for future studies.

THE IMPORTANCE OF SECURITY FOR E-BUSINESS AND E- ENTREPRENEUR

Globally, smartphone markets are growing every year and diverse smartphone models, operation systems, and applications are being developed. Smartphones have the advantage of being small in size but have high computing capacity to the extent that they are regarded as portable computers, and they can be utilized for diverse purposes by configuring users' own customized devices through various applications.

Since various companies develop applications and sell in application markets, such as Play Store (Google) and App Store (Apple), revenue can be also generated by loading advertisements on individual applications. The current trend in e-business and e-entrepreneur is a move to mobile devices.

However, applications containing malicious codes are not the only things being distributed illegally, sensitive information such as personal information and payment information is being leaked. The damages are increasing with the increase in the smartphone trends. Therefore, security for smartphones is becoming an issue.

Android aspires to more open environments than the other operating systems to allow more convenient communication among applications. Therefore, many related vulnerabilities exist. In particular, the permission system is the likely to be misused.

The purpose of the present paper is to analyze attack models that may occur in the Android permission system to explore vulnerabilities and offer suggestions for improving the situation.

PRELIMINARIES FOR ANDROID

Applications

Different from their ancestors, the powerfulness and flexibility for smartphones including Android are largely built on applications. An Android application is an archive file (.apk, Android package) containing its components, resources and a manifest file. The manifest file contains information about all the static components, the permission requirements and the other descriptions of the application.

An application on Android is isolated from other applications by its unique Linux user ID. It has its own storage space and runs

Supporting Innovation Through Knowledge Management in the Extended Enterprise

Mikel Sorli and Dragan Stokic (2008). *Information Technology Entrepreneurship and Innovation (pp. 310-328).*

www.igi-global.com/chapter/supporting-innovation-through-knowledge-management/23643?camid=4v1a