Chapter 5

IMPACT OF USER DATA PRIVACY MANAGEMENT CONTROLS ON MOBILE DEVICE INVESTIGATIONS

Panagiotis Andriotis and Theo Tryfonas

Abstract There are many different types of mobile device users, but most of them do not seek to expand the functionality of their smartphones and prefer to interact with them using predefined user profiles and settings. However, “power users” are always seeking opportunities to gain absolute control of their devices and expand their capabilities. For this reason, power users attempt to obtain “super user” privileges (root) or jailbreak their devices. Meanwhile, the “bring your own device” (BYOD) trend in the workplace and increased numbers of high profile users who demand enhanced data privacy and protection are changing the mobile device landscape. This chapter discusses variations of the Android operating system that attempt to bypass the limitations imposed by the previous Android permission model (up to version 5.1) and highlights the fact that forensic analysts will encounter devices with altered characteristics. Also, the chapter discusses the Android permission model introduced in the latest operating system (version M or 6.0) that will likely change the way users interact with apps.

Keywords: Android devices, privacy, trust, power users, anti-forensics

1. Introduction

Android is an open source project that enables developers to alter operating system characteristics according to their preferences. Data privacy and the lack of user controls on installed apps have always been major concerns for security-aware developers and users. The previous – but still dominant – permission model of Android operating systems (up to version 5.1) has been criticized for limiting the ability of users to control the private data that apps may access.
This chapter focuses on mobile devices that run variations of the Android Open Source Project (AOSP). It highlights the various approaches that deal with the fact that the previous – but still dominant – permission model of Android operating systems (up to version 5.1) is not flexible and does not allow users to restrict access to specific resources. Furthermore, it demonstrates that evidence derived from devices may contain falsified data due to app utilization that employs obfuscation measures to protect user data and privacy. This fact raises the specter that the probative value of “evidence” extracted from such devices can be put into question.

2. Data Privacy Concerns

Contemporary mobile devices are equipped with many sensors. The Android documentation lists at least twenty variables (e.g., TYPE_ACCELEROMETER) that can be used by developers to access various sensors and enrich the functionality of their apps. The sensors are essentially divided into hardware- and software-based sensors. Apps normally use sensors to measure orientation, motion and other environmental conditions and provide the expected functionality to users. A portion of the data produced by the apps contains information derived from sensors. This information is stored internally on the device or in the cloud. Some of the information may be encrypted (e.g., locations from Google Maps).

For example, a call to the camera or microphone of an Android device requires the inclusion of the appropriate permissions in the manifest xml file from the developer so that a user can be informed about the resources required by the specific app. Next, the user has to decide if he/she will accept the stated policy and download the app from the Play Store. The previous Android permission model has a binary accept-reject character. Therefore, if an app needs access to a user’s contact list, it has to ask the user for permission to access it; then, the user is informed that his/her contact list will be shared via content providers to other ecosystems. Figure 1 presents screenshots of Android’s privacy management control variations (left to right: permissions, incognito mode and Privacy Guard).

In theory, the Android permission model assures that data privacy is not violated without the knowledge of the user. But this is not always the case. In fact, privacy in the smartphone ecosystem is not only related to the stored data accessible by third-party applications via the aforementioned route, but privacy is also associated with the sensors themselves. For example, an Android device does not require permissions to be declared by an app for access to a number of device sensors.