Chapter 22
A Privacy Protection Approach Based on Android Application's Runtime Behavior Monitor and Control

Fan Wu
Beijing University of Posts and Telecommunications, Beijing, China

Yuan'An Liu
Beijing University of Posts and Telecommunications, Beijing, China

Ran Sun
Beijing University of Posts and Telecommunications, Beijing, China

Feng Liu
State Key Laboratory of Information Security, Institute of Information Engineering and School of Cybersecurity University of Chinese Academy of Sciences, Chinese Academy of Sciences, Beijing, China

Wenhao Fan
Beijing University of Posts and Telecommunications, Beijing, China

Hui Lu
Guangzhou University, Guangzhou, China

ABSTRACT

This article proposes a system that focuses on Android application runtime behavior forensics. Using Linux processes, a dynamic injection and a Java function hook technology, the system is able to manipulate the runtime behavior of applications without modifying the Android framework and the application's source code. Based on this method, a privacy data protection policy that reflects users' intentions is proposed by extracting and recording the privacy data usage in applications. Moreover, an optimized random forest algorithm is proposed to reduce the policy training time. The result shows that the system realizes the functions of application runtime behavior monitor and control. An experiment on 134 widely used applications shows that the basic privacy policy could satisfy the majority of users' privacy intentions.

DOI: 10.4018/978-1-7998-2466-4.ch022

INTRODUCTION

Background

Nowadays mobile phones are widely used in communications, and in many other aspects in people's daily lives as well. Personal information, including many kinds of privacy data, has been saved in users' mobile phones and used by installed applications on the phone. Research from Zscaler (Maritza, 2016) reveals that, in each quarter, about 0.4 percent of the mobile device transactions are leaking privacy data, including device metadata, location and personally identifiable information. In reality, many applications overuse the privilege that users grant prevalently. Privacy leaks and privilege abuse have become severe problems in mobile security. Given this, it is imperative to concern about the privacy data forensics and protection of mobile phones, since they are no longer a simple mobile device for communications, but an essential data storage tool for almost every mobile phone user.

Malware detection is a prevalent method to prevent the user's privacy leaks, which in fact contains a lot of work of digital forensics. One of the works includes detection consists of detecting whether applications have been repackaged, collected user privacy data or consumed fees silently. However, malware detection cannot be the only benchmark to prevent privacy leaks, since many benign applications may also abuse the users' privacy data. Furthermore, many forensic works have determined that privacy data is leaked only when its metadata is sent out of the phone, and they don't consider that privacy data might be utilized inside the applications. Mobile-phone operating systems currently provide only coarse-grained controls for regulating whether an application can access private information (Enck et al., 2014). However, they cannot control applications' behavior when a privacy leak happens.

Considering the drawbacks mentioned above, it can be concluded that privacy data is a matter of grave importance to users. Any behavior that accesses privacy data of an application is vital, and should therefore be under surveillance or provide user-notice, regardless of whether or not the application itself is malicious.

In this paper, an application behavior forensics and privacy protection system for Android based on the applications' runtime behavior is designed. The system is capable of monitoring any application's runtime behavior which accesses privacy data on Android, thus providing forensic evidence of privilege abuse and possible privacy leaks. Based on the captured runtime behavior, the system is able to enforce a rather fine-grained privacy policy that controls the source of privacy data.

RELATED WORK

Most approaches of mobile digital forensics are more or less based on applications' behavior analysis, namely the information flow tracking technique, because privacy source data is mainly utilized by various applications installed on Android devices. An application's behavior analysis mainly falls into two categories: static analysis and dynamic analysis. The former keep watch on the complete program code and all possible paths of execution before runtime, whereas the later looks at the instructions executed in the program-run in real time (Lokhande, & Dhavale, 2014).