International Journal of Digital Crime and Forensics
Volume 12 • Issue 3 • July-September 2020

User Identity Hiding Method of Android

Yi Zhang, Institute of Information Engineering, Chinese Academy of Sciences, China

ABSTRACT

With an 86.1% global market share, Android takes the top spot smartphone operating system. Due to its open environment, Android suffers from various kinds of attacks, which cause a serious privacy leakage problem. To protect users' privacy information, this article proposes a user identity hiding method of Android. The method constructs a hidden user identity in Android based on the multi-user mechanism. In particular, by hiding information related to hidden user, the method makes it invisible to normal user. The method can quickly switch the identity of normal user and hidden user by passwords. Thus, the method can deal with privacy information under hidden user identity while processing regular information under normal user identity. Compared with traditional security methods of Android, this method significantly improves the security of android devices without arousing any suspicion. Experimental results show the effectiveness of the method that it not only achieves ideal hiding effect on user identity, but also implements quick switch without sacrificing the performance of system.

KEYWORDS

Android, Multi-User, User Identity Hiding

INTRODUCTION

Nowadays, smartphone is widely used in large variety of areas, such as communication, shopping online, map navigation, getting latest news, etc. which make it an integral part of people's lives. Thus, a great deal of privacy information in smartphones, such as payment accounts, bank statement, personal photo, location information, address book and so on, become one of our most valuable treasure. Accordingly, malicious attacks on the privacy information of our smartphone are growing fast year by year. As the most widely used intelligent mobile operating system on market, Android is the primary target of all kinds of malware attacks (Xu et al., 2016). Considering the great value of privacy information stored in our phones, it is of great significance to investigate on different measures of improving the security level of Android devices.

To protect users' privacy information, researchers adopt a method of multi-system isolation in Android devices. It provides multiple running environments on a single physical device, which are independent and do not interfere with each other. By providing isolated environment for secret information, it can protect users' privacy effectively. In recent study (Huber et al., 2015), the authors propose a security architecture for Android devices based on operating system-level virtualization technology. Nevertheless, the security architecture requires deep customization for Android system, making it very complicated to implement. The "Platinum" phones of Coolpad use hardware isolation

DOI: 10.4018/IJDCF.2020070102

technique to achieve dual-system through two different ROMs (Techweb, 2017). However, the technique requires hardware customization, which is not fit for common models. In general, the traditional multi-system methods mainly focus on providing an independent and secure operating environment for users' privacy information, but it also tells attackers that users' privacy information is stored in the security system. In fact, there are very few ways to cover up the running environment of multi-system. So, it is easy to arouse suspicion when multi-system technology is used as privacy protection method. Besides, the switch of multi-system is usually complicated which may seriously impact users' experience.

In addition, smartphone manufactures design a variety of confidential cabinets and private spaces to store users' privacy information. For example, the mobile phone of Huawei provides a confidential cabinets function. Users can use it to store secret files like pictures, audio, video and so on. Only users who know the password of confidential cabinets will be able to see the secret files, but it tells attackers the existence and exact position of secret information. Once attackers crack the password of the confidential cabinets, he can directly obtain users' secret information.

In this paper, we propose a user identity hiding method based on Android device to protect users' privacy information. The method implements dual-system on mobile phone based on the multi-user mechanism of Android system. Compared with the multi-system of mobile phone with virtualization technology, our method is simple to implement and has little impact on system performance. Compared with hardware isolation technology of the "Platinum" phones, our method is implemented on software level. So it is independent to specific hardware devices, which makes it more flexible and applicable to different makers of smartphones. Furthermore, our dual-system method can make the storage of the users' regular information and privacy information further isolated from each other. The method constructs a hidden user identity, which is invisible to normal user. One can deal with privacy information under hidden user identity while processing regular information under normal user identity. Even malware detection cannot find users' privacy information through conventional detection methods. In general, this paper's contributions are:

- We develop a new kind of dual-system on mobile phone based on the multi-user mechanism of Android system to protect users' privacy. Compared with the multi-system of mobile phone with virtualization technology and hardware customization, our dual-system method is more convenient and effective without sacrificing the performance of the system;
- We construct a hiding method to achieve the identity of hidden user is invisible to the normal user. The method can prevent the conventional detection approach and common logical technique from obtaining users' privacy information. Thus, the method significantly improves the security of android devices without arousing any suspicion;
- We realize the quick, secure login and switching function between dual users. In addition, we improve the security of users' privacy information through the behavior monitoring and data encryption.

The rest of the paper is organized as follows. In Section 2, we will present some related work on privacy protection measures of Android system. Section 3 shows the design of our method. In Section 4, we present the experimental results and analysis of the proposed method. Finally, the paper is concluded in Section 5.

RELATED WORK

In recent years, privacy protection of Android has become a hot issue and main concern of researchers and mobile phone manufacturers, which is drawing more and more attention from all over the world. Researchers have put forward a variety of solutions in the privacy protection problem of Android.