Who Leaks Our Information

Yan Zhuang[1], Fan Hu[1], Jiajie Huo[1], Qing Zhao[1], Suzhai Wang[2]
[1]Humanities College Tianjin Agricultural University, Tianjin, 300384, China
[2]College of Marxism Tianjin Agricultural University, Tianjin, 300384, China

Abstract: Mobile phones play a very important role both at work and in life. On the one hand, mobile phones are our indispensable good helpers; on the other hand, mobile phones have become a serious threat to the security of our personal information. We often encounter such problems, such as the content searched by one kind of software is presented in another software, when a certain demand is mentioned during the call, the relevant pushes will be seen. So, how does mobile software leak our information? What are the consequent hazards and hidden dangers? What attitude do we have to face this behavior?

Keywords: Android phone; software permissions; personal information security

1. Introduction

Smart phones are in complete harmony with our lives, and various software is our rightful assistants to meet our needs. However, the leakage of personal information in recent years has become an invincible threat to us. Since 2011, 1.127 billion users' privacy information has been leaked, including basic information, device information, account information, privacy information, social relationship information, network behavior information and so on. Man-made reselling information, PC infection, website vulnerabilities, and mobile phone vulnerabilities are the four major ways for personal information leakage. (quoting Baidu) Many people have lost money and important information because of this, and they have been plagued by spam and telemarketing from time to time. Nowadays, this phenomenon is very common and seriously threatens our lives. More and more people begin to attach importance to this problem and hope that it will be improved.

The research on information leakage has existed for a long time. The literature elaborates the security hidden risks of mobile Internet in detail, and makes supplementary research on the four aspects of mobile Internet access environment security, transmission network security, device security and service security. The literature focuses on the privacy leakage under the Android platform, focusing on location information, through ant colony algorithm and location weighting algorithm, the harm of users' information leakage is concretized, and the ways of privacy leakage are analyzed in depth. In the literature, based on the application of privacy leakage detection technology on Android platform, the current research situation and progress in this field are introduced, and the evaluation criteria for the current evaluation criteria of privacy detection technology are proposed. The above scholars' research has all about the information leakage of smart phones users and put forward effective solutions. This paper also studies users' privacy leakage, but it focuses on mobile software access rights and their impact, and proceeds from the following aspects.

2. Access Rights of Mobile Phone Software

2.1. What are the permissions

In the phone settings, we know the permissions are: dialing, sending SMS, sending MMS, accessing contacts, accessing call records, accessing SMS/MMS, adding/deleting contacts, locating mobile phones, accessing mobile phone identification code, accessing schedule, using the camera, recording, turning WLAN on/off, turning Bluetooth on/off, calling transfer, installing applications, reading installed application information.

2.2. Why does it request authorization

In the first case, the use of some functions does require access to the appropriate permissions. For example, communication software needs to read the address book to achieve the purpose of communication.

In the second case, in order to obtain greater benefits or prepare for future benefits, such as entertainment software collects users' preference information, on the one hand, for upgrading and improving their own software; on the other hand, for selling or sharing information; unrelated software acquires permissions, such as weather software requests to access the address book, etc., to prepare for the future operation of the software.

3. How to Leak Users' Privacy

The first case is that the applications send users' data to development companies. When using the application software, users will leave traces on them, and personalized settings will leave their own information. In order to provide better services, the application software will also encourage users to set their own modes. The applications transmit the feedback information of users' preferences to the development companies. On the one hand, the development companies can better match the users' preferences and improve the applications quality; on the other hand, the development companies can negotiate with other companies based on the data and seek common interests. The second case is that data sharing among applications. What we know is that different applications of the same software development company can share users' data, which is generally acceptable to us, but if different applications of different development companies exchange information with each other, that's another matter.

4. Hazards and Hidden Risks

Here we do not study the collection of users' data for good intentions to improve software performance and to better serve users. We focus on the harm and hidden risks of malicious collection of users' data.

Location information: First, the time of stay. Development companies or third parties can speculate on our life laws based on our staying time in different locations. Usually, the places we stay during the daytime are mostly work places. The places we stay at night are homes or temporary residences; depending on the change of our staying time during the holiday, it can speculate that we are traveling or visiting home. It can judge whether we are local or not, and lay the foundation for the judgment of next step. Second, the location and nature of the work unit. According to the location information, it can be determined which places the users are working in, such as government departments, large enterprises, business centers and so on. Based on this, the users' financial resources, status, and the value of users' information can be judged. Compared with ordinary users, the information leakage of government staff is more harmful, the impact will be greater, which not only affects the individuals, but also leaks the state secrets.

Mobile phone model: Mobile phone model is an important basis for development companies and third parties to judge users' financial resources and consumption concepts. They provide users with very targeted advertising pushes according to it.

Record of shopping list: Online shopping records are the best and most accurate medium for reflecting our personal preferences and needs. We often find that when you buy online, there will be similarly viewed products that will be pushed the next time you open the software, and even similar products will be promoted in the browser. So how do browsers capture our needs? There are many similar incidents. For example, after we talk to our friends about where we want to travel, where we have been uncomfortable recently, and how we feel, we will receive relevant ticketing, hotel, medical treatment and various articles about chicken soup for the soul in different applications, which shows that our information has been leaked. Criminals can use location information to speculate about our life patterns, such as when they are at home and when they are at work, and can use this information to steal, or to harm users on the road. Criminals can also judge the nature of users' work based on the above information. If the user is an important person, the loss will be immeasurable to the user itself and others. Even ordinary people have huge hidden dangers. We don't know when and where someone will be watching us on the other end of the cell phone, stealing our information and waiting for the opportunity to act. On the one hand, this kind of behavior seriously violates our right to privacy and even threatens our personal safety, which is a violation of the law and a disregard for citizens. On the other hand, this kind of behavior is becoming more and more serious in the market. Criminals uncontrollably collect and disclose user information. In the short term, it seems to be beneficial to orientate the market more accurately, which not only saves costs but also increases profits. However, in the long term, such behavior will lead to the decline of the entire industry, which will have a major impact on China's economic and technological development, and will seriously hinder the pace of our industry towards the world. Users, even the country, will be deeply affected

5. Solutions

The country and relevant departments must formulate laws to restrict the development of such enterprises, so that enterprises can have laws to follow. At the same time, the state and relevant departments must increase the punishment for criminals and unscrupulous enterprises, and they will punish criminals severely. Contents should include access issues for software development companies, boundaries between personal privacy and user information, and penalty criteria for disclosing users' privacy. Relevant enterprises should consider the long-term development of enterprises and improve their deficiencies. The collection of user's data is strictly based on the operational needs of the software, and does not violate the boundaries of the law, and the enterprise must strictly protect the user's data and bear corresponding responsibilities. Users should always be vigilant, refuse bad applications, cancel the corresponding permissions immediately after using them, and be cautious when the software gains the permissions granted. At the same time, the mobile phone should not store important information in order to avoid being stolen and used by criminals to cause user losses.

6. Conclusion

On the one hand, we hope that through investigation and research, the consequences of personal information leakage can be more concrete, more directly reflected to people, and force people to raise their awareness of privacy security, and protect their privacy; on the other hand, it has aroused the attention of relevant parties and prompted relevant departments to solve this problem; in another aspect, it can warn operators, software developers, criminals, etc. We firmly defend our privacy rights and do not allow others to leak our personal privacy in any form. Ultimately, we want to build an environment that is more orderly, safer, and faster for software applications.

5. Acknowledgment

College students innovation and entrepreneurship training program (No. 201807016).

References

[1] Zhang C. Research on Mobile Internet Privacy Leakage, Master's Thesis, Beijing University of Posts and Telecommunications, 2013.

[2] Li X. Research of the Privacy Leakage on the Android Platform Master's Thesis, Henan University of Technology, 2016.

[3] Li Z.Q., Wang Y.N. Software, 2017, 38, 10, 77-82.