IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 2, February 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

A Study on Personal Information Risk in Mobile Applications: A Case Study in Korea

Hyang-Mi Park[1], Ji-Yeon Yoo[2]

[12]Department of Information and Security Management
Sangmyung University
Seoul City 03016, Republic of Korea

Abstract

Due to the mobility and connectivity of mobile devices, most activities for work and everyday life are now handled on mobile platforms. And while the use of mobile applications to facilitate such processing and activities is expanding, there is a growing concern about privacy exposure and privacy breaches.

In this study, we look at the personal information risks and countermeasures in mobile applications, analyzing the situation in Korea, which has a high mobile penetration rate. To do this, we compare the application rights of 300 applications in the Google Play Store, analyze the possible risks in mobile applications through the Australian and US mobile app guidelines, and suggest solutions.

Keywords: *Mobile Application, Personal Information, Mobile App Guidelines, Mobile-related Regulations, Free Applications*

1. Introduction

The number of smartphone users worldwide is expected to exceed 5 billion by 2017, and it is expected that mobile communication and linkage between information, people, and objects will be further expanded as more people enter the hyperconnected society. In the midst of this, the use of mobile applications to expand and utilize mobile functions is rapidly increasing.

In Korea, the use of mobile applications is increasing exponentially. The use of smartphones in Korea According to a survey by the Ministry of Creation Science and the Korea Internet & Security Agency (KISA), smartphone usage in 2016 was 84.6%, up from 39.2% in 2011[1]. Smartphone users in Korea have installed an average of 48 mobile apps on average each, and they used 21.7% of installed apps of average in the past month [2].

These statistics demonstrate that smartphone users in Korea are actively using mobile applications. Meanwhile, in November 2014[1], it was reported in the airwave news that personal information had been leaked through a flashlight application. The article was based on a report [3] that compared and analyzed a total of 10 flashlight applications, focusing on the threat of privacy infringement from flashlight applications that require a collection of poisonous privileges.

In this paper, we expect that not only flashlight applications, but also other categories of applications, could cause privacy infringements like those described in the circumstances above. So that developers can understand the range of authority that they can exercise regarding the information that they require from the individual users of their applications, we will conduct a survey of mobile users in Korea and analyze their disclosure of personal information in downloading, installing and using applications.

[1] MBC News. The problem was that flashlight applications steal personal information; the user may not know, or may even believe that they have turned off the collection of personal information.

2. Precedent research

Kim, Ik-hwan and Kim, Tae-hyun (2011)[4] stated that "it is possible to access information such as the phone number of the device and the serial number of the USIM according to the privilege of the application and this information may be leaked to the outside through the network. The potential security risks can be reduced." In addition, Huh, Hwang Seok, Kang Sung Hoon and Kim Seung-joo (2013)[5] said, "If unnecessary privileges are assigned to the purpose and function of the Android app, or if the privilege increases due to the implementation problem of the app, inappropriate behavior occurs, information can be exposed to the outside world."

In this paper, we investigate and analyze cases of overuse or out-of-privilege usage of personal data.

3. Investigation and analysis

3.1 Overview

In this study, we analyzed the applications in the Google Play Store to determine the personal information required to download and install mobile applications. To conduct

the survey, we chose the category of 'Tools,' which includes 'Games,' 'Communication,' and various other utilities, according to the ranking of the types of main-use mobile applications selected in [2]. In total, we analyzed 50 authorized [editor's note: do you mean paid?] applications and 50 free applications and classified the information they require as mandatory authority, optional authority, or other authority items.

The required and/or optional items of authority classified in this paper are shown in Table 1 below. In the case of the 'Game' category, the authority to store and update the settings of the application and the need to identify the user were selected as mandatory items. Apps in the 'Communication' category are intended to communicate with other people, so it is almost always essential that developers have the authority to associate with users' personal accounts and store their contacts and other information. It is difficult to delineate all the essential items of authority in the 'Tools' category due to the varied characteristics of these applications, which include system elements such as anti-viral software and backup applications and utilities including keyboard, alarm, and memo-based applications. We did determine that broadly, mandatory authorities included the authority for basic storage and the right to network access.

Table 1. Required / Optional by Category

	Required items	Selected items
Games	- Photos / Media / Files -Wi-Fi connection information -ID	- In-app purchases -Etc
Communication	-ID -address book - Photo / Media / File	- Network data setting -location -SMS -Cell Phone -Wi-Fi connection information - Device ID and call information -Etc
Tool	※ It is difficult to specify mandatory authority items due to category characteristics.	- Device and app history - Photo / Media / File -Wi-Fi connection information -Etc

3.2 Results of analysis

Table 2 shows the average number of privileges required from users according to categories. As a result of analyzing the authority of mobile applications, three conclusions could be drawn. First, the scope of authority required to download and install mobile applications is against the principle of minimal collection. Second, free applications require more privileges than paid applications. Third, the consent process for downloading and installing the application is performed in a single act or 'lump.'

First, as can be seen in Table 2, the developer's choices regarding the information required to download and install mobile applications accounts for the largest percentage of required items. This evidence supports the conclusion that the scope of information the average developer desires to collect through the initial request for authority exceeds the required level. Also, it should be noted that the need for more than the necessary authority can be used as a channel to leak personal information. The 'Other' item, which comprehensively covers the items that are not authorized by the Google Play Store, can include the authority to use a location information provider for 'Modify System Settings,' 'Internet Dialing,' 'Full Network Access,' and 'NFC Control.' It provides room for the developer to arbitrarily control a smartphone independently from the user's will.

Table 2. Average Entitlements Required by Category

	Game		Communication		Tools	
	Paid	Free	Paid	Free	Paid	Free
Total items	6.5	10.3	8.4	16.8	7.5	11.5
Required items	3.0	3.0	3.0	3.0	-	-
Optional items	3.5	7.3	5.4	13.8	7.5	11.5

Second, research suggests that free applications require more privileges than paid applications. This implies that the developers of free applications consider the acquisition of personal information and its economic value, not money paid upfront, as their primary reward for releasing free applications. However, users are often unaware of the fact that their personal information is used in this manner.

Third, it is often the case that users seeking to download an app - free or paid - must consent to provide a large amount of personal information or authority before the application can even be used. This results in the same violation of the principle of minimum collection. This consent-to-collection system, which is contrary to the "Personal Information Protection Act," can be seen as a violation of the user's right to self-determination of personal information[1].

[1] Article 22 (4) of the 「Personal Data Protection Act of Korea」, "When receiving the consent of an information entity regarding the processing of personal information … it should distinguish between personal information that can be processed without the consent of the information entity and personal information requiring the consent of the information entity."

4. Analysis and Implications of Guideline of Major Countries

III. We will analyze Korea's "Guidelines for Privacy Protection of New Media Services" and the corresponding guidelines of the United States and Australia, focusing on the problems presented in the survey and analysis, and present directions for mobile-related guidelines in Korea.

4.1 Korea

The "New Media Service[1] Privacy Guidelines" not only protect personal information on smartphones but also guide service providers and users about the entire range of new media services. Article 3, Section 1, Paragraph 3 of these guidelines addresses the minimum collection principle but does not include items on selection agreements or the risk of infringement of personal information in new media.

4.2 United States

In the United States, "Marketing your mobile app: Get it right from the start," offers a number of things application developers should follow to protect the personal data of their users, covering privacy considerations, transparency, how best to collect personal information, and how to protect the privacy of children under the age of 13. These guidelines propose minimum collection principles in a way that mentions collection principles, management, and use and destruction according to the lifecycle of information, but does not include guidance on other optional agreements or the risk of infringement of personal information.

4.3 Australia

Australia's "Mobile Privacy Guidelines" state that if users need to consent to the collection and use of their personal information, they should be clear of the purpose of the collection of that information and ensure they understand the relevant information to prevent violations of the principle of minimum collection. Also, according to the Australian Privacy Act, mobile application developers are only allowed to collect the personal information necessary for the provision of the application or service. It is prohibited to collect personal information without the consent of the user. In particular, the act of collecting and storing sensitive information, location information, and the address book, etc. of the user is prohibited, and the operation of the terminal camera without consent is also prohibited. To prevent problems caused by collective consent, it is necessary for developers to notify users of the status of personal information use in real time by determining the appropriate time to request the consent for personal information collection.

[1] New media services: cloud computing services, social network services, social commerce services, smartphone utilization services

5. Conclusion

Through the investigation and analysis above, we have proposed that both mobile application users and developers need to change their actions and attitudes. First, since the institutional systems for protecting users are currently insufficient, when an application user downloads and installs the mobile application, they should consider the authority required by the developer's side. In this way, users are continuously aware of the risk of application privilege. To facilitate this, information protection organizations should periodically provide training and guidelines for protecting individual's personal information on their mobile phones.

At the same time, mobile-related regulations should be strengthened. To solve the problems presented above, the consent system in the mobile world should be divided into required consent items and optional consent items, as it is on the internet. It is clearly necessary to continuously improve efforts to prevent personal information from being leaked by the users of the mobile application and their respective developers.

References

[1] Korea Internet & Security Agency (KISA), “Internet Usage Survey by 2016.”
[2] Korea Internet & Security Agency (KISA), “Mobile Internet Survey in 2015.”
[3] SnoopWall, “Flashlight Apps Threat Assessment Report,” 2014.
[4] Kim, I. and Kim, T., “Design and Implementation of Flexible Application Program Authority Management in Android Platform,” The Korea Information Processing Society Transactions, Part C, Vol.18, No. 3, pp.151-156, 2011.
[5] Huh, S., Kang, S. and Kim, S., “Proposing Security Verification Stages for Implementation of Secure Android Applications”, The Korea Information Processing Society Transactions, Vol.2 No.10, pp.445-460, 2013.
[6] About Google play application permissions
[7] Korea’s Ministry of Government Administration and Home Affairs, “New Media Service Privacy Guidelines", Ministry of Public Administration and Security,” 2012.
[8] Federal Trade Commission, “Marketing your mobile app: Get it right from the start,” 2013.
[9] Korea’s National IT Industry Promotion Agency, “Australian Government, Mobile App Privacy Guideline Announcement,” International ICT R & D Policy Trend Vol.7, pp.50-63, 2013

First Author Hyang-Mi Park is currently enrolled in a Masters degree in Graduate School, Sangmyung University. Her research interests are in

areas of Information Security, IT Management System, and Personal Data Protection.

Corresponding Author Ji-Yeon Yoo is currently a Professor of Sangmyung University. She received her Ph.D. in Information Management Engineering from Korea University. Her current research interests include Data Protection Strategy, Digital Risk Management, and Cyber Security, etc