Proposal of Security Evaluation System using User's Reviews and Permissions for Android Applications

Naonobu Okazaki
University of Miyazaki,
1-1 Gakuen-Kibanadai-Nishi, Miyazaki, 889-2192, Japan

Yoshihiro Kita
Kanagawa Institute of Technology,
1030 Shimo-Ogino, Atsugi, 243-0292, Japan

Kentaro Aburada
Oita National College of Technology,
1666 Ooaza-Maki, Oita, 870-0152, Japan

Mirang Park
Kanagawa Institute of Technology,
1030 Shimo-Ogino, Atsugi, 243-0292, Japan
E-mail: oka@cs.miyazaki-u.ac.jp, y.kita@ccy.kanagawa-it.ac.jp,
aburada@oita-ct.ac.jp, mirang@nw.kanagawa-it.ac.jp

Abstract

Leakage of the personal information in Android OS powered device by mal-applications is becoming the heavy matter. The Android OS users must be careful not to install mal-applications. The reviews and the using permissions of applications are useful by users to detect mal-application. However, the most of users read the reviews only. All users must be cautious about not only the using permissions but also the combination of them. In this paper, we propose the security evaluation system to prevent the installation of mal-applications on Android OS. This system indicates the user reviews with the using permission information of application to new users.
Keywords: Security for applications, Mal-applications, User's reviews, Permissions, Android OS.

1. Introduction

Recently, leakage of the personal information in Android OS powered device by mal-applications is becoming heavy matter. Google implements mal-application detection system "Bouncer" for Google play[1]. However, mal-applications are not eliminated completely, even how to defeat Bouncer legally has been found also.

Google Play provides the using permissions of application to users when downloads there. The users not read the permissions, because it is need to consider combination of permissions, and have specialized knowledge for permissions.

The most of the users get the information of application from user reviews. A part of exist reviews is useless review that is the malicious review or the unrelated review to contents of the application. There is the problem that it is difficult to determine the mal-application by users using the existing user reviews.

In this paper, we propose the security evaluation system using user reviews for Android OS. This system

shows the user reviews with the using permission information of application to new users. New user evaluates the one of reviews, and determines to download or not download the application. The evaluation of the review is transmitted to reviewer. The reviewer refers to the evaluation of review for next review.

2. Preceding Studies

Reviews are useful as guidelines for new users to download the application. However, if the mal-application developer writes the review of the application in order to be installed it by users, this review is exaggerated review or fake review. The other users trust these review, and are suffered damage by mal-applications.

It is impossible to remove the vulnerability of applications completely, but guidelines of secure applications for Android developers (i.e. iSEC Partner[2]) are issued by various organizations for security information.

Existing review system (i.e. Google play[1]) show reviews of user and using permissions to new users. It is possible to predict the risk of application from reviews and permissions, because these are indicate the behavior of application. But, users can not understand the risk of application adequately, because these are not indicate the risk of application in combination with other permissions, and it is difficult to understand the behavior of application by users who do not understand the expertise of security and function of mobile terminals.

Matsudo[3] proposed security advisor system, which indicates the risk of application by the combination of permissions. This system shows the number of download and the risk level of application to new users. However, these values are not objective and fair measure, because other users can manipulate these values intentionally, and new users do not have information enough to determine the application downloading by these values only. It needs for new users to show the user's reviews of applications in order to get the information of applications.

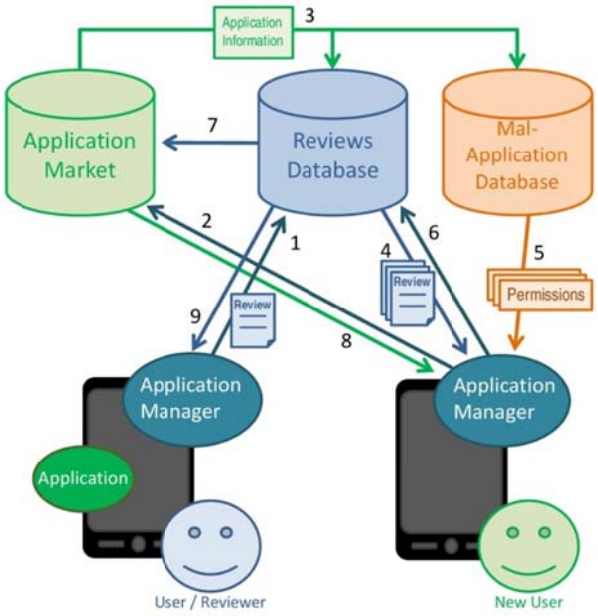

Fig. 1. Structure of security evaluation system.

3. Security Evaluation System

We propose security evaluation system, which indicate the risk of application by the reviews and using permissions. This system indicates the reviews and the evaluation of them. Fig.1 shows the structure of security evaluation system. This system consists of three parts as follows:

- Reviews Database
  This is storage of reviews and the evaluation of reviews, which are sent from all users.
- Mal-Application Database
  This is the storage of permissions and the information of mal-applications (i.e. application's name, version, developer).
- Application Manager
  This is the application which indicates the reviews and the risk of applications by the combination of permissions to terminal user, and transmits the user's review to review database.

Table 1. Risk allowances of applications.

	Safety	Caution	Danger
Does the application have the one or more dangerous permission?	NO	YES	YES
Does the application have the dangerous combination of permissions?	NO	NO	YES
Is the application reported as mal-application?	NO	NO	YES/NO

Table 2. The permissions concern the personal information or the information leak.

Permissions concern personal information	Permissions concern information leak
READ_CONTACTS	INTERNET
WRITE_CONTACTS	SEND_SMS
READ_CALENDAR	BLUETOOTH
WRITE_CALENDAR	NFC
READ_LOGS	USE_SIP
BIND_APPWIDGET	CHANGE_NETWORK_STATE
READ_PROFILE	BLUETOOTH_ADMIN
WRITE_PROFILE	
ACCESS_FINE_LOCATION	
ACCESS_COARSE_LOCATION	
ACCESS_MOCK_LOCATION	
GET_ACCOUNT	
READ_EXTRNAL_STORAGE	
WRITE_EXTRNAL_STORAGE	

The procedure of this system is described as follows:

1. The user which is using the application sends a review to review database through the user's application manager.
2. New user requests the download of the application to the application market.
3. The application market sends the information of the application (i.e. name, developer, request user's name) to reviews database and mal-application database.
4. Reviews database shows the all review and the evaluation of them for the application to new user through the new user's application manager.
5. Mal-application database shows the information of using permissions and the information of mal-application to new user.
6. New user gives the evaluation “Good” or “Bad” for the one of the reviews, and reports the evaluation of the review to reviews database through the application manager.
7. Reviews database stores the evaluation of review, and permit the download of the application to application market.
8. New user downloads the application to application market through the application manager.
9. Reviews database reports the evaluation of the review to existing user as reviewer.

Reviews have two types: positive reviews and negative reviews. Positive reviews include selling points or good features for the application. Negative reviews include wrong points or problems of the application. The reviews are evaluated not only new users but also existing user instead of writing the review.

The permissions have the four protection levels[4]: “normal,” “dangerous,” “signature,” and “signatureOfSystem.” Table.1 shows the risk allowances of applications that we defined. We divide the risk of applications into three levels as follows according to the protection levels and the combination of permissions.

- Safety
  All permissions use the protection level “normal” only.
- Caution
  Permissions use the protection level “dangerous,” “signature,” or “signatureOfSystem.”
- Danger
  The application is permitted the functions which include both connecting internets and accessing the personal information, plus the condition of “Caution.”

Table.2 shows the permissions concern the personal information or the information leak. The applications include these permissions are allocated the risk of applications “Danger.”

Fig.2 shows the example of indication for risk allowances of applications. The application manager indicates the risk of the application using the kinds of

Fig. 2. Example of indication for risk allowances of applications.

three colors for each risk and descriptions of the using permissions. The new users can recognize the dangerous applications easily by these indications.

4. Consideration

New users can understand the behavior of applications in detail by the reviews. It is important for all users to understand the risk of application correctly. It needs to show the reviews and the risk of combination of using permissions for new users to determine the application downloading. Table.3 shows the indication of each method. Google play does not indicate the risk of combination of using permissions. Security advisory system does not show the reviews of users. These methods are insufficient to prevent the installation of mal-applications. Security evaluation system indicates the reviews and the risk on combination of using permission. Therefore, security evaluation system is useful method for new user to prevent installation of the mal-application.

However, all of the dangerous applications are not the mal-applications. It is difficult for users to recognize the mal-applications from all of the dangerous applications even if they use the security evaluation system. It needs to improve security evaluation system to recognize the mal-application more exactly.

5. Conclusion

We proposed security evaluation system using user reviews for Android OS in order to prevent installation of the mal-application. This system indicates the reviews, the evaluation of review, and the risk of combination of using permissions. The reviewer refers the evaluation of the reviewer's review, and will be written the useful review next time. Therefore, new users can recognize the mal-applications by useful reviews and the indication of risk for installing the applications.

References

[1] Google play, Google. http://play.google.com/store
[2] J. Burns, Developing secure mobile application for android, *iSEC Partners* (2008).
[3] T. Matsudo, E. Kodama, J. Wang, and T. Takata, A proposal of security advisory system at the time of the installation of applications on Android OS, in *Proc. 15th Int. Conf. Network-Based Information Systems (NBiS)* (2012), pp.261-267,
[4] B. M. A. Egner and U. Meyer, Messing with android's model, in *Proc. the 2012 IEEE 11th Int. Conf. Trust, Security and Privacy in Computing and Communications* (2012), pp.504-514.