Protect Local Data on Personal Devices: Third Party Application

Teejan T. El-Khazendar*, Tawfiq S. M. Barhoom

Information Technology, Islamic University of Gaza, Gaza, Palestine

Email address:
telkhazendar@gmail.com (T. T. El-Khazendar), tbarhoom@iugaza.edu (T. S. M. Barhoom)

Abstract:
Android became an important device all over the world. Android customers download many applications from play store to get services or desired benefits, or entertainment. Android applications include various permissions. These permissions are implemented by developers in the code during the application development. Therefore, the developers can access personal data of the user's device when the user download these applications and accept the downloading terms and conditions. Further, the user has to accept these terms and conditions to be able to download the applications without knowing the risk of accepting these terms and conditions. This result arises from allowing the developer to access their personal data, which harm their privacy. Otherwise, the user may seriously understand the danger from accepting the terms and conditions which allow the developers to access permissions for their personal data; consequently, he cancels the downloading process of the application. So, customers either have to accept terms and conditions which harm their personal data or they have to decline these terms and conditions which prevent them to enjoy the use of these applications. The main purpose of this work is to propose a solution to this problem. The proposed solution is that google has to limit the feature that let the developers add these permissions during coding for the applications except these permissions are required to the applications; the developers have to ask google for adding permissions and justify their request.

Keywords: Android, Security, Personal Data, Local Data, Third-Party, Permissions

1. Introduction

Android operating system is an open source software stack run by Google built in several devices such as mobile and tablets. Its operating system is governed by the mobile device's capacities. Safety is a main part of any Android device. Some android applications protect your personal data and blocks wicked applications from Google play before installing them. The android operating system is built on Unix. The launch of Google’s Android introduced enormous numbers of users to these markets. Google's android Market managed the progress of android devices because it offers a vast number of applications accessible to Android users [1].

Operating systems include printed programs which are written by developers other than the owner of the operating system and named third party applications. As an example, Microsoft® systems include many applications. First party application is any program developed by Microsoft. Third party applications are any program developed by a different person [2].

Information security is significant due to the substantial amount of work on the technical resistances such as encryption and firewalls joined with shielding information and invasion recognition systems [3].

A combination of two implementation mechanisms is applied by android to protect data and applications from destruction. The first mechanism is at the system level and the second one is at the inter-component communication level [4].

Android applications can be classified according to benefits and damage into three main types. The first one is the best type of applications which gives us benefit or entertainment without harming our privacy or containing any viruses. The second type is the malicious type of applications which is kind of cyber-attack. The third one of applications gives us the desired benefit but it has some permissions which by accepting them we lose the confidentiality. The focus of our study is on the third type of applications and how to fix the problem of violating the privacy resulting from downloading it [5].
However, there are a vast number of downloads from Android Market on some popular applications encompass damaging permissions for the customer personal data. The customers allow downloading without under-standing the danger of accepting these permissions because they lack the visibility into how applications use their private data. This means that there should be a method to allow users to download the applications without violating their privacy and keep the confidentiality of their local data.

In this paper, we will discuss the problem arises from using unmalicious applications which violate the user's confidentiality. Then, we will propose a solution to solve this problem. The paper is organized as follows. Next section is dedicated to software development kit and permission. The topic of the third section is request errors from developers. The focus of section four is on access control models. Android operating system Security is presented in section five. Section six introduced the related work and art State. In section seven, advanced permission manager approach is described. Finally, the conclusion is given in section eight.

2. Software Development Kit and Permission

Android software development kit (SDK) allows developers to create applications for android platform. Developers can indicate any permission as an application. The permissions are categorized for the following four defense stages that are added in the manifest.xml file during the application development [4]:

1. Normal permission: any application can call this type of permissions built in its manifest.xml file.
2. Dangerous permission: this type of permissions is allowed only after the user approval.
3. Signature permission: This type is allowed only for specific type of applications signed by the owner of the platform.
4. Signature or system permission: this type performance is similar to the signature permissions; however, it makes heritage matching between the new system and the previous system.

Another delegation tool URI permission is presented. These permissions are necessary for database archives as critical competences.

3. Request Errors

Sometimes, the reason for asking unneeded permissions is clear. This is due to developers error where developers ask inessential permissions for names seems linked to the task of their applications, but they are not the desired permissions.

Delegate is an application, which sends a request to different deputy application inquiring the delegate to do an action. When the delegate calls application programming interface having a defense permission, the delegate demands a permission; however, the transmitter of the request does not need permission [6].

4. Access Control Models

There are two kinds of access control models: compulsory access control and optional access control. The access control can be classified into these two kinds depending on their role. Osborn et al. [7] offered logical structures for both of the two types of access control patterns to determine the access control type by means of the role-based access control.

In the role-based access control, permissions and roles are connected; moreover, users are given the roles’ permissions as members of proper roles, which make permissions management easier.

Users can be easily moved from any role to different one. New permissions can be allowed for roles and permissions can be withdrawn from roles as needed. Security officer is allowed to strongly vary the status of a role and the regular users permitted to start that specific role by delivering run-time demands [8].

5. Android Operating System Security

Operating system: The Android platform comprises the following five core strata [9]:

1. Applications: This layer consists of applications only installed on it. Examples of these applications are messaging applications, games, browser etc.
2. Application Framework: This layer offers high-level services to applications. The developers are permitted to use application framework elements such as Content Providers, Views, and Manager in order to construct their applications to implement on Android Kernel.
3. Libraries: There is a set of libraries on top of Linux kernel. Libraries encompass open-source Web browser engine WebKit, SQLite database used for storage and distribution of application data, Secure Sockets Layer (SSL) libraries in authority of Internet security etc.
5. Linux Kernel: This affords elementary system utilities such as device management, process management etc.

Security: There are a lot of access control tools delivered by Linux. Users are the basic part of these tools. Linux permission tools control android application and system files. The system or root user can sign to system files. Application users can sign to application files. Files produced by a specific application are not allowed to be accessed to different applications except explicitly indicated.

The security application level is the permission application tool. This tool can be used by developers to impose constraints on particular processes that can be accomplished by an application. There are about 100 permissions integrated by android to manage actions. Additional permissions can be announced by android developers [10].
6. Related Work and Art State

Greveler [11] offered an approach of focal information. The goal of this approach is to create cloud information that is coded and packed by usage rule. When the information entered, it will refer to its rule, then, make simulated atmosphere, and evaluate the credibility of the information atmosphere.

Shedding the light on benign application, Fahl et al. [12] studied safety coercions imposed by benign Android applications. These applications legally develop confidentiality associated with user information such as official papers. Further, they presented MalloDroid tool to discover possible weakness.

Operating systems of some mobiles permit consumers to govern the admission to critical data. Therefore, previous authors [13] presented a novel tool named TaintDroid. This tracking tool is data stream which able to track several sources of serious information over third party applications.

Earlier research [14] suggested an approach by means of python scripts and numerous implements that repeatedly repack android application to insert a safety correspondent when the application uses personal information.

Pinapps.com [15] implemented and published an innovative android application named PermissionDog on the Play Store. This application permits users to view permissions in the applications on their personal devices. Depending on these permissions, it defines how harmful the application to the users privacy.

7. Advanced Permission Manager Approach

A recent implemented application approach called advanced permission manager is published by SteelWorks [16]. This application is an authorization administration tool considered to surf installed permissions applications; furthermore, it permits users to edit and eliminate permissions of applications files.

Figure 1 illustrates schematically the advanced permission manager approach. This implemented application allows users to edit the permissions on their devices. When the customers click on the app icon, the screen lists all the installed applications. Then, they can choose any one of the desired applications. Next, a new window shows all the permissions of the selected application. So, the customer is allowed to select or deselect any permission.

Therefore, Android users will be able to download the desired applications and get the benefit from it without allowing them to harm their personal data. Moreover, this kind of applications requests the user to allow the application's developers to violate his confidentiality during downloading these applications. As a result of that, the customers still do not have an ideal solution.

Therefore, we suggest on google to impose restrictions on the developers during writing their algorithms for the applications. These restrictions prevent the developers from adding unnecessary permissions; moreover, they help customers to keep their confidentiality.

8. Conclusion

In this paper, we reviewed the critical permissions problem which face the android users. The advanced permission manager approach is briefly described. It is shown that the users are able to edit the application's permissions by deselecting the unwanted permissions, which harm the user's privacy. However, the users still have permission problems because the advanced permission manager application's developers are able to violate their privacy. Consequently, we ask google to limit the application developers' authority to harm the confidentiality.

References


