THE SOFTWARE TOOL FOR IDENTIFYING THE CELLULAR NETWORK STATUS OF A MOBILE DEVICE UNDER THE ANDROID OPERATING SYSTEM

Hunko Mykhailo, Voropaeva Ksenia
Scientific advisor - Candidate of Technical Sciences, Associate Professor
Tkachev Vitalii
Kharkov National University of Radio Electronics
14 Nauky ave., Kharkov, 61166
Department of Electronic Computers, tel. (057) 702-13-54
E-mail: hunko@ieee.org

The task of developing a software package to determine the occupancy of the communication line is relevant and in demand today. For this development it is not enough only to develop the program, also dangerous permissions are needed. This publication deals with the specifics of granting permissions.

In order for the Android cellular network occupancy application to work correctly, you need to grant permissions. A little more detail about permissions and granting permissions in Android OS. The Android operating system is designed in such a way that in order to perform certain operations or access certain resources, the application must have permission to do so.

Some permissions require more attention than others. Some of them, like accessing the Internet and stopping background processes, belong to the «normal» category, because they are not dangerous for the user.

Others, such as accessing the calendar and contacts, recording audio, using wearable sensors, and reading data from external storage, are considered dangerous.

Users of Android 6.0 and newer versions can choose which permissions to give to apps after they are installed. In earlier versions, there was no choice. Cybercriminals have learned to use this to their advantage.

Now that security loophole has been closed. As of August 1, 2018, Google requires apps to be compatible with an Android version at least 8.0.

Since app permissions must be granted before installation, it's important to know how they can affect privacy. There are nine groups of dangerous permissions. If a user grants or denies one of the permissions in a group, that choice extends to the other permissions in the same group.

The groups are:

- wearable sensors;
- calendar;
- camera;
- contacts;
- location;
- microphone;
- telephone;

- SMS;
- memory.

For the application to work correctly, one of the prerequisites is the condition of granting permissions. For this application it is necessary to grant permissions to the Internet and contacts.

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example.applicationtest">

    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.READ_CONTACTS" />
    <uses-permission android:name="android.permission.WRITE_CONTACTS" />
    <uses-permission android:name="android.permission.BLUETOOTH" />
    <uses-permission android:name="android.permission.CAMERA" />
    <uses-permission android:name="android.permission.SEND_SMS" />

    <application
        android:allowBackup="true"
        android:icon="@mipmap/ic_launcher"
        android:label="@string/app_name"
```

Fig. 1 - Example of granting permits

It is also worth noting that permissions must be written in the manifest and requested in the Runtime.

Additional features of mobile app development, such as resource optimization, testing, and publishing the app to the Google play console are suggested for further publications.

References:

1. Vitalii Tkachov, Anna Budko, Kateryna Hvozdetska and Daryna Hrebeniuk. Method of Building Dynamic Multi-hop VPN Chains for Ensuring Security of Terminal Access Systems // IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T): Kharkiv 06-09 oct. 2020, Kharkiv.

2. Tkachov, V., Bondarenko, M., Ulyanov, O., & Reznichenko, O. (2019, December). Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT) (pp. 161-165).

3. Tkachov, V., Hunko, M., Volotka, V.: Scenarios for Implementation of Nested Virtualization Technology in Task of Improving Cloud Firewall Fault Tolerance. In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), pp. 759-763. IEEE (2019).