Composition of the information security methods for a smart environment and the research

Nerijus Šatkauskas
Department of Computer Sciences
Kaunas University of Technology
Kaunas, Lithuania
nerijus.satkauskas@ktu.edu

***Abstract*—Smart devices and the smart environment itself is getting more and more popular. A big part of smart devices uses the Android operating system. Since any information on these devices can become available to the third parties on the basis of granted permissions, it is very important to consider it properly before granting them. A permission monitoring system prototype has been proposed for this purpose.**

***Keywords*—dangerous permission group, dangerous permission, information leakage, android operating system, smart environment, smart device, information value, information sensitivity, Android permissions, permission monitoring**

I. Introduction

Smart environment is rather an abstract conception and it may refer to a number of more specific areas in question. If we referred to one of many definitions for the smart environment, it would sound like [1] “ordinary environments equipped with visual and audio sensing systems, pervasive devices, sensors and networks that can perceive and react to people…”. It is expected that the number of such devices will only increase in the future.

One of the smart devices which makes a big part of the smart environment is a smartphone. A dominating operating system currently is Android [2]. This operating system has been created by Google on the basis of Linux. The operating system due to its nature of being an open source one has to be well controlled and maintained in order to keep it as safe as possible.

The purpose of this research is to analyze security issues the Android operating system faces. It assesses the security of the smart environment information storage in the Android operating system. It attempts to detect whether any unauthorized parties can get access to this information. The methods which may strengthen the security are considered.

A prototype has been proposed for this purpose. This prototype shall classify the tested applications based on their permissions which suggest any potential information leakage. The results will be compared with some other applications which are currently available on the Play Store for the same purpose.

II. SMART ENVIRONMENT THREATS

Mobile devices once were considered as safe ones but everything has changed as soon as operating systems were introduced. Installing an application is not only an additional comfort. It can be an additional concern as well. Especially if it is a malware which can leak any information. IoT environment or the smart environment in this particular case since the issues are rather common can be divided into three main levels [3]: application level, transportation level and perception level. All these three levels bear threats which are typical to them.

TABLE I. SMART ENVIRONMENT THREAT LEVELS

Layer	Main Threats
Application level: provides customer requested services like air temperature	Data leakage: stealing data
	DoS attacks: making services unavailable
	Malicious code injection: exploiting known vulnerabilities
Transportation level: transmits and receives any collected data	Routing attacks: intermediate malicious nodes
	DoS attacks: making nodes unavailable
	Data transit attacks: attacks in networks
Perception level: physical sensors to collect any data and to process it	Physical attacks: node tempering, replacing
	Impersonation: fake identity for attacks
	DoS attacks: making nodes unavailable
	Routing attacks: intermediate malicious nodes
	Data transit attacks: sniffing, man-in-the-middle

This research focuses on the application level. The operating system Android is picked due to its leading positions in the market.

III. ANALYSIS OF THE CURRENTLY AVAILABLE ANDROID DATA LEAKAGE MONITORING TOOLS

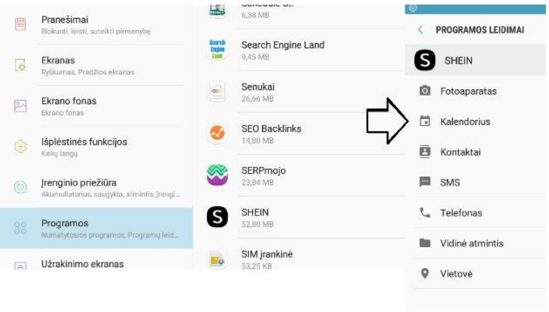
Data availability to third parties in the Android operating system relies on the permission model [4]. Permissions are such labels which should be assigned by developers to their application. The application must define in the manifest file which sensitive resources it needs to have access to. The user during the installation has a chance either to grant these permissions or not.

A. *Preinstalled permission manager*

As Android 6.0 “Marshmallow” has been introduced in 2015, the ability was provided to toggle any granted dangerous permission groups for any specific application [5]. The accessibility of this tool may vary depending on the manufacturer of a device, but it can be accessed in general via Settings > Apps / Application Manager > Permissions.

A screenshot is provided below of the operating system Android 8.1.0. It gives access to the list of all the installed applications. Dangerous permission groups can be reviewed, granted or revoked at any time.

However, if a user has no previous knowledge about the permissions, the list may not always be informative enough.



Pranešimai
Blokuoti, leisti, suteikti pirmenybę
Ekranas
Ryškumas, Pradžios ekranas
Ekrano fonas
Ekrano fonas
Išplėstinės funkcijos
Kelių langų
Įrenginio priežiūra
Akumuliatorius, saugykla, atmintis, įrengi...
Programos
Numatytosios programos, Programų leid...
Užrakinimo ekranas

6,38 MB
Search Engine Land
9,45 MB
Senukai
26,66 MB
SEO Backlinks
14,80 MB
SERPmojo
23,84 MB
SHEIN
52,80 MB
SIM įrankinė
53,25 KB

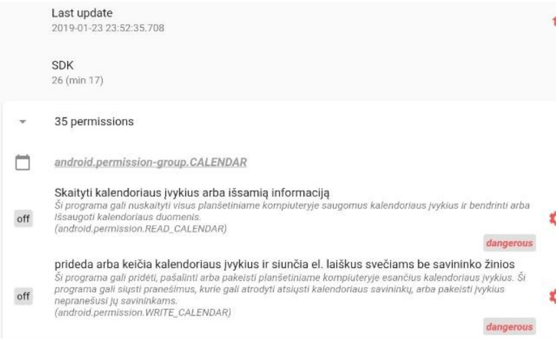
PROGRAMOS LEIDIMAI
SHEIN
Fotoaparatas
Kalendorius
Kontaktai
SMS
Telefonas
Vidinė atmintis
Vietovė

Fig. 1. Preinstalled permission manager

B. *Application Inspector*

A good alternative which is available on Play Store for the permission management is Application Inspector. This is a third-party application which is developed by UBQSoft.

The tool once it is launched provides a list of all the installed applications. One can see more details after picking any particular application within that list concerning libraries, last update time etc. Involved permissions are described as well as their level they belong to is provided: dangerous, normal, signature. The status of granted or not granted is available which can be changed after tapping and being directed to relevant Settings submenus.



Last update
2019-01-23 23:52:35.708

SDK
26 (min 17)

35 permissions

android.permission-group.CALENDAR

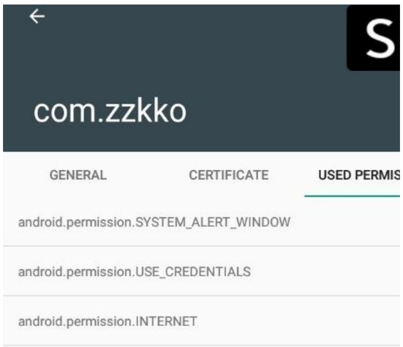
off
Skaityti kalendoriaus įvykius arba išsamią informaciją
Ši programa gali nuskaityti visus planšetiniame kompiuteryje saugomus kalendoriaus įvykius ir bendrinti arba išsaugoti kalendoriaus duomenis.
(android.permission.READ_CALENDAR)
dangerous

off
prideda arba keičia kalendoriaus įvykius ir siunčia el. laiškus svečiams be savininko žinios
Ši programa gali pridėti, pašalinti arba pakeisti planšetiniame kompiuteryje esančius kalendoriaus įvykius. Ši programa gali siųsti pranešimus, kurie gali atrodyti atsiųsti kalendoriaus savininkų, arba pakeisti įvykius nepranešusi jų savininkams.
(android.permission.WRITE_CALENDAR)
dangerous

Fig. 2. Application Inspector

C. *Apk Analyzer*

It is a very extensive analyzer and it provides access to different statistical data after a specific application is picked within a general scanned applications list. There is a tab for used permissions. These permissions are listed after tapping the tab, but the information resources are very limited. There are no descriptions about these permissions. It is undefined which level they belong to. There is no information if any of these permissions in the manifest file are granted or not.



com.zzkko

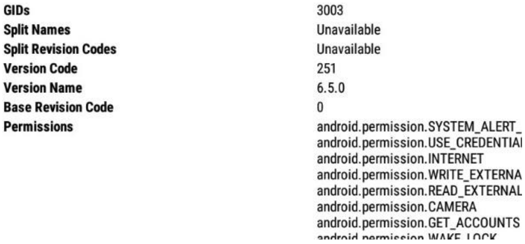
GENERAL CERTIFICATE USED PERMIS

android.permission.SYSTEM_ALERT_WINDOW
android.permission.USE_CREDENTIALS
android.permission.INTERNET

Fig. 3. Apk Analyzer

D. *PackageInfo*

Another application which can be helpful for scanning any installed applications on the device is PackageInfo. It gives a list of applications after scanning which are available for a more detailed review after picking any of them. It gives some package information, including the list of permissions. There are no detailed descriptions of these permissions. The state whether they are granted or not is unidentified.



GIDs	3003
Split Names	Unavailable
Split Revision Codes	Unavailable
Version Code	251
Version Name	6.5.0
Base Revision Code	0
Permissions	android.permission.SYSTEM_ALERT_ android.permission.USE_CREDENTIAl android.permission.INTERNET android.permission.WRITE_EXTERNA android.permission.READ_EXTERNAL android.permission.CAMERA android.permission.GET_ACCOUNTS android.permission.WAKE_LOCK

Fig. 4. PackageInfo

It becomes obvious after the analysis of some currently available tools for permission scanning and monitoring that the focus given on the permissions may not be enough for a regular user. A regular user may not want to search for any explanatory information about the granted permissions in external sources. It may lead the user to underestimating any potential threat due to personal information leakage.

IV. V-S AXIS INFORMATION SENSITIVITY ASSESSMENT

Different data classification methods were taken into consideration but V-S method [6] was chosen as the most appropriate one in this case. This method classifies any available information based on 2 axes which stand for information value and sensitivity. As the authors suggest who have introduced this method, it is possible to assign the data to different information classes while implementing different security measures.

A. *V-S axis method in the prototype*

In order to able to use the proposed V-S axis method for the data on Android device, we first need to define the value of the vertical axis for information **sensitivity (*Y*)**. Sensitivity axis has tree levels: low (0), middle (1), and high (2).

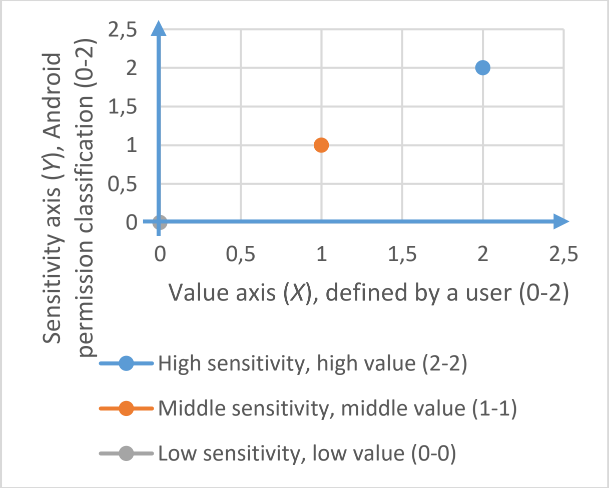


Fig. 5. V-S axis chart

The horizontal axis for information **value (*X*)** has also three levels. These levels are correspondingly: low (0), middle (1), and high (2).

The official classification of permissions available on Android developers' portal was used for that purpose [7]. Permissions are classified there into four groups: normal, dangerous, signature, and special ones. This official classification reflects different information sensitivity levels to any potential information leakage. These permissions were assigned to the **sensitivity (*Y*) axis** in the following manner:

1) *Low (0):* Normal permissions are assigned to this level due their low potential threat. These permissions are granted to any installed application on a smart device without any intervention on the user side.

2) *Middle (1):* Some normal permissions are assigned to this level. Applications with these permissions may cause some inconvenience to users like CHANGE_NETWORK_STATE which allow to change the connectivity to wireless networks.

3) *High (2):* Dangerous permissions groups were assigned to this level. It is officially confirmed and classified as having negative impact once the information which belongs to the above class is unintentionally exposed to any third part parties.

Signature permissions and special permissions were not further considered in this research. Therefore, they were not assigned to any axis level.

The **horizontal (*X*) axis** for information value is used for a personal assessment of the information stored on the smart device. The values for this axis are selected by default in the prototype but a user can change them any time.

1) *Low (0):* This information is not valuable to the user or the user will not have any significant issues upon losing it. Permissions of low sensitivity (*Y*) axis level are matched to this value (*X*) axis level by default which results in 0 as a score.

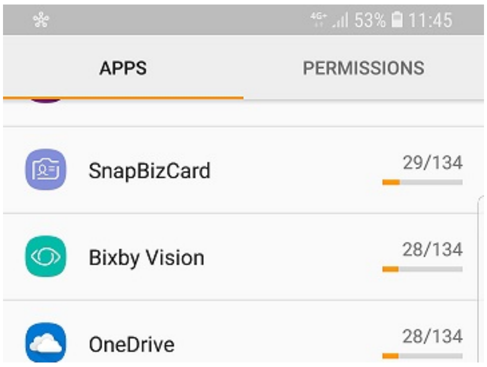
2) *Middle (1):* This information might have some value to the user or the user might have some issues upon losing it. Permissions of middle sensitivity (*Y*) axis level are matched to this value (*X*) axis level by default which results in 1 as a score.

3) *High (2):* This information is valuable to the user. Losing it might cause considerable issues or financial losses. Permissions of high sensitivity (*Y*) axis level are matched to this value (*X*) axis level by default which results in 4 as a score.

B. *Proposed prototype based on V-S classification*

The proposed prototype Permission Monitoring System gives a quick review of the installed applications. It consists of 2 main lists. The first one is made of applications which are sorted in the order of the highest danger point score to the lowest one. A total danger point score for a specific application is compared to the maximum possible danger point score (maximum point score is 134). It gives that way a quick review of the data leakage potential.

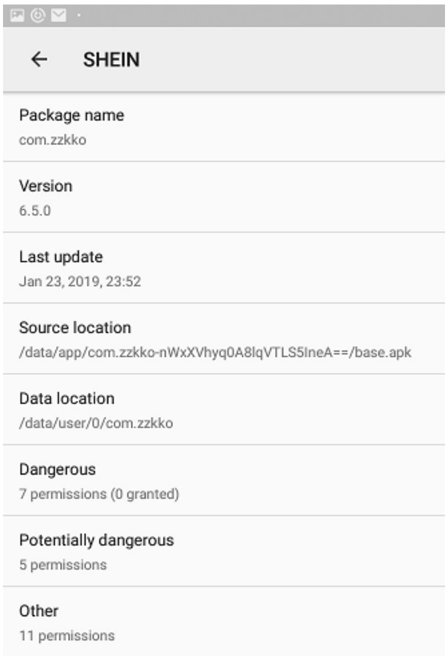
V-S axis classification method is used both for the maximum danger point score calculation and for the current danger point score calculation of any specific application. As mentioned above, permission classification and default information values which a user can adjust to his / her own priority any time are taken into consideration.



SnapBizCard	29/134
Bixby Vision	28/134
OneDrive	28/134

Fig. 6. Permission Monitoring System

If a user taps any application in the application list provided by the prototype, further options are available. The user can see the package name, version number, last update time etc. It also provides the number of dangerous, potentially dangerous and normal permissions. These permissions can be further explored after tapping their titles in this submenu.



Package name
com.zzkko

Version
6.5.0

Last update
Jan 23, 2019, 23:52

Source location
/data/app/com.zzkko-nWxXVhyq0A8lqVTLS5lneA==/base.apk

Data location
/data/user/0/com.zzkko

Dangerous
7 permissions (0 granted)

Potentially dangerous
5 permissions

Other
11 permissions

Fig. 7. Specific application data

As soon as a submenu option for permissions is tapped, one can see the dangerous permissions which of them are namely granted. If these dangerous permission groups are not granted, but they are still in the list, it means that the manifest file contains that permission group, and as the application is used, sooner or later this permission group will be requested by the corresponding application. It is also the place where a user can change the value (horizontal one) axis level to a preferred one if he / she thinks that the default value does not meet his / her expectations. E.g. if a user feels that there is no important information in his / her contacts book and exposing it unintentionally to any third parties is not a big concern, it is possible to change the value axis level to the middle one or the low one. Danger point score will be recalculated accordingly. As the recalculation is completed, the score can accordingly be higher or lower.

C. V-S classification of permissions

The following default values were used to calculate the score for any permission used within an application.

TABLE II. MAX. OF POINTS FOR A SPECIFIC PERMISSION

Dangerous permissions	2	0	2	4
Potentially dangerous	1	0	1	2
Normal permissions	0	0	0	0
		0	1	2
		Low value	Average value	High value

The maximum amount of points for a **dangerous** permission is 4. Meanwhile, the maximum amount of points for **potentially dangerous** permissions is 2.

The following formula was used to calculate the danger point score:

$$(Y_D * X_D) + (Y_{PD} * X_{PD}).$$

D means in this formula “Dangerous permission”, meanwhile *PD* means “Potentially dangerous”. *Y* and *X* are the names of the axes.

All the permission groups which belong to the dangerous protection level are used for this prototype. As it was mentioned above, they belong to level High (2) on the sensitivity (*Y*) axis. Further details are provided below.

TABLE III. PERMISSION GROUPS AND MAX. POINT SCORE

Permission group	**Permissions and max. score on both axis**			
	Permissions	***Y_D***	***X_D***	***Multiplication***
CALENDAR	READ_CALENDAR	2	2	4
	WRITE_CALENDAR	2	2	4
CALL_LOG	READ_CALL_LOG	2	2	4
	WRITE_CALL_LOG	2	2	4
	PROCESS_OUTGOING_CALLS	2	2	4
CAMERA	CAMERA	2	2	4
CONTACTS	READ_CONTACTS	2	2	4
	WRITE_CONTACTS	2	2	4
	GET_ACCOUNTS	2	2	4
LOCATION	ACCESS_FINE_LOCATION	2	2	4
	ACCESS_COARS_LOCATION	2	2	4
MICROPHONE	RECORD_AUDIO	2	2	4
PHONE	READ_PHONE_STATE	2	2	4
	READ_PHONE_NUMBERS	2	2	4
	CALL_PHONE	2	2	4
	ANSWER_PHONE_CALLS	2	2	4
	ADD_VOICEMAIL	2	2	4
	USE_SIP	2	2	4
SENSORS	BODY_SENSORS	2	2	4
SMS	SEND_SMS	2	2	4
	RECEIVE_SMS	2	2	4
	READ_SMS	2	2	4
	RECEIVE_WAP_PUSH	2	2	4
	RECEIVE_MMS	2	2	4
STORAGE	READ_EXTERNAL_STORAGE	2	2	4
	WRITE_EXTERNAL_STORAGE	2	2	4
Maximum point score for dangerous permissions				104

Some normal protection level permissions are used for the sensitivity (*Y*) axis with the default value set to Middle. These values officially are considered as not dangerous, but a user may find it uncomfortable if their status becomes uncontrollable. Therefore, the level on the sensitivity axis (*Y*) is 1, and the level on the value axis (*X*) which can be changed by a user is also 1 by default. However, this default value is considered as 2 when calculating the maximum danger point score. The following table provides further calculation details.

TABLE IV. MAX. SCORE FOR POTENTIALLY DANGEROUS

Permissions	**Y_{PD}**	**X_{PD}**	**Multiplication**
CHANGE_NETWORK_STATE	1	2	2
CHANGE_WIFI_STATE	1	2	2
MODIFY_AUDIO_SETTINGS	1	2	2
REQUEST_DELETE_PACKAGES	1	2	2
NFC	1	2	2
REORDER_TASKS	1	2	2
REQUEST_INSTALL_PACKAGES	1	2	2
FLASHLIGHT	1	2	2
GET_TASKS	1	2	2
BILLING	1	2	2
SET_ALARM	1	2	2
DISABLE_KEYGUARD	1	2	2
SET_WALLPAPER	1	2	2
SYSTEM_ALERT_WINDOW	1	2	2
WRITE_SETTINGS	1	2	2
Maximum point score for potentially dangerous permissions			30

TABLE V. TOTAL MAXIMUM SCORE

Maximum danger point score	Max. score
Maximum point score for dangerous permissions	104
Maximum point score for potentially dangerous permissions	30
Maximum point score for dangerous permissions + potentially dangerous permissions	**134**

The maximum danger point score therefore is 134. If a user changes the level on the value (*X*) axis for any dangerous permission group or a potentially dangerous permission to low, it means that this permission will be multiplied by 0 which leads this permission to be unconsidered in the total danger point score for applications.

V. EXPERIMENTAL FINDINGS

The purposes of completing information leakage experiments based on permissions were the following ones:

1) Which categories do pose the highest risk of an information leakage among the tested ones?

2) Which applications do pose the highest risk of an information leakage among the tested ones?

3) Which permissions are requested the most frequently?

The following devices were used in one or other way in order to download the applications for testing them with the prototype.

TABLE VI. USED DEVICES

Device	Basic specifications
Lenovo Yoga 530	Windows Pro 10 Intel® Core™ i3-8130U CPU @ 2,20 Ghz 16,0 GB RAM
Samsung Galaxy S8	Android 8.0.0 Octa-core (2.3GHz Quad + 1.7GHz Quad), 64 bit, 10nm processor 4 GB RAM (LPDDR4)
Samsung Tab A (SM-T585)	Android 8.1.0 Octa-core (4x1.6 GHz Cortex-A53 & 4x1.0 GHz Cortex-A53) 3 GB RAM

Applications were downloaded based on different categories. Applications within the categories were picked while using the most popular application list since these applications are the most relevant ones to the biggest number of users.

The most popular 20 applications from the categories below were downloaded and installed.

- Shopping
- Finance
- Communication
- Education
- Business

Tested categories according to the results of the information leakage risk are distributed on the chart in the following way.

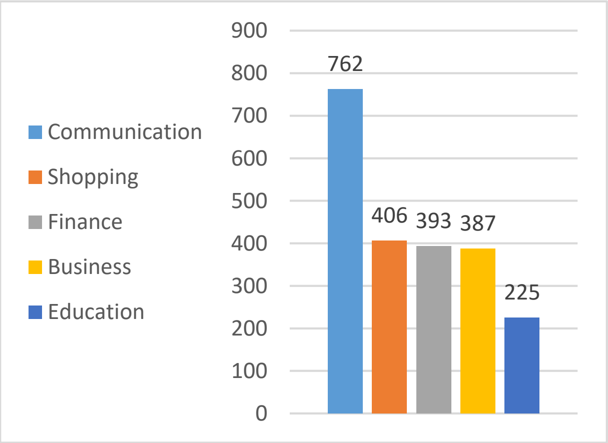


Fig. 8. Distribution of the tested categories

The results were calculated by summing up the danger point score of all the tested applications within that category. It was 20 top applications in it based on their popularity.

The following applications pose the highest risk of an information leakage among the tested ones.

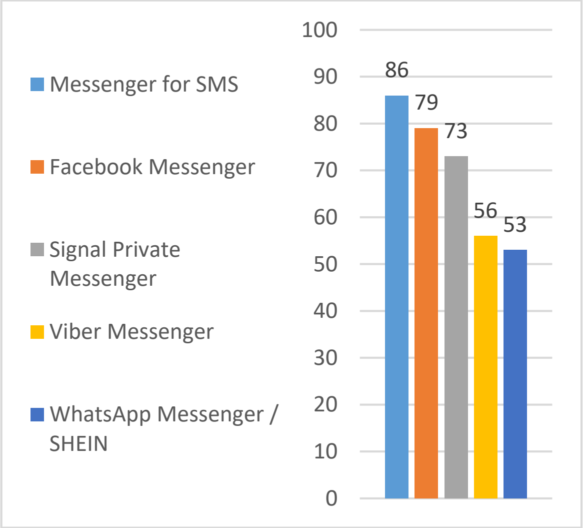


Fig. 9. The most dangerous applications

These applications were picked by looking for the highest danger point score among all the tested applications. The number of the tested applications is 100 at the moment.

The following dangerous permissions which are in chart below are requested the most frequently by the downloaded applications which were used for this research.

Numbers of the usage of different dangerous permissions were calculated in this test. As 100 Android applications were currently tested in this research, the chart numbers suggest the amount of instances the corresponding permission was requested or was to be requested. It means in this case that the permission READ_EXTERNAL_STORAGE was requested by 78 applications out of 100 tested applications. Top 5 permissions with the highest usage number were picked. It suggests which information has the highest leak potential.

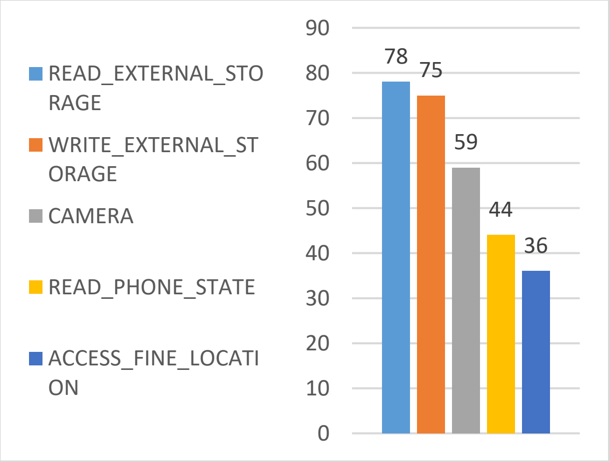


Fig. 10. The most frequent permissions

VI. CONCLUSIONS

Android OS security is based on the permission model. However, granting the permissions can be underestimated by a regular user due to a lack of available information or interest in his/her personal security.

A prototype has been offered which provides a simple risk assessment of any information leakage. A user does not need to have any awareness of permissions to understand the results.

There is an option to cancel any granted permission but after it is cancelled, an application may not work correctly.

100 applications in total from 5 different categories were tested. The results are provided in charts for a comparative purpose.

REFERENCES

[1] (2006) ACM DIGITAL LIBRARY, “State of the art smart spaces application models and software infrastructure”. [Online]. Available: http://ubiquity.acm.org/article.cfm?id=1167869

[2] (2017) IEEEXplore, “Critical Review of Static Taint Analysis of Android Applications for Detecting Information Leakages”, 8th International Conference on Information Technology (ICIT). [Online]. Available: http://ieeexplore.ieee.org/document/8080041/

[3] (2017) IEEEXplore, “Evaluating critical security issues of the IoT world: Present and Future challenges”. [Online]. Available: http://ieeexplore.ieee.org/document/8086136/

[4] (2017) IEEEXplore, “Android Permissions Unleashed”. [Online]. Available: https://ieeexplore.ieee.org/document/7243742

[5] Google Play Help, “Control your app permissions on Android 6.0 and up”, [Online]. Available: https://support.google.com/googleplay/answer/6270602?hl=en-GB

[6] (2007) IEEEXplore, “Research on Supply Chain Information Classification Based on Information Value and Information Sensitivity”. [Online]. Available: http://ieeexplore.ieee.org/document/4280248/

[7] (2018) “Protection levels”. [Online]. Available: https://developer.android.com/guide/topics/permissions/overview#normal-dangerous