Android Information Leak Potential in Benign, Malware, and Commercial Spyware Applications

Nerijus Šatkauskas[#1]

Department of Computer Sciences , Kaunas University of Technology
Kaunas, Lithuania

Abstract

There are well over 2 billion smartphones currently in the world. Their number is only increasing.A big part of OS is Android. It is not only an OS with huge resources. Android is notorious for an increased information leak potential. Information availability is based on granted permissions, but a user may underestimate it due to a lack of interest or skills. Application developers are often blamed for asking too many permissions. Meanwhile malware and commercial spyware means that the information leak in question is uncontrollable.

Permission Management System, the prototype, has been offered which gives a simplified review of any potential information leak due to permissions. A comparative study has been completed on benign, malware and commercial spyware applications.

Keywords *— Android, permission,dangerous permission, information leak, smartphones,permission monitoring, permission management, benign, malware, commercial spyware*

I. INTRODUCTION

As soon as smartphones emerged, they have become an inseparable part of our lives. It is said that the number of currently used smartphones in the world is well over 2 billions [1]. The comfort they give though is not for free. It comes at a price. And we pay with our privacy for this.

There were severalOSfor smartphones since their introduction but few of them survived up to the current day. One of these OS is Android.It was 2008 when the first device was launched with it. Ever since, it is getting bigger, more powerful and more popular. Now it is more than a smartphone OS. It is available in wearable electronics, IoT, TV boxes etc.

Plenty of scientific studies have been completed due to Android OS privacy concerns. Google Play Store is a relatively safe place for downloading any application. They have a variety of security procedures to check the uploaded applications. However, there were some reports that a malware is not always removed on time to prevent users from getting infected. And repackaged applications seem to be the easiest method to inject any malicious code into an application which looks like an original one. One study claims that about 86 % of malware samples [2] were repackaged applications.

It is not only malware which is know for information leakage to third parties. Benign Android applications are also notorious for this. One can hear such claims like “Google trades privacy and security for… [3]”. In addition to this, there are plenty spying applications which cantransmit your location, messages, calls and other data. The primary goal of spying applications is to monitor your children or to keep track of businesssmartphones [4] as it is officially suggested, but the truth is they are often used to spy on somebody you may have an access to his/her devices to configure it for, and it can be a victim in this particular case [5].

This research aims to analyze any information leak potential the Android OS faces throughout the usage of different applications. It will focus on the methods of the information leak, and the type of data which can be made available to any unauthorized persons.

The experimental part includes a prototype which was used to test the applications. Benign and spying applications were downloaded from Google Play Store and their official dealers, meanwhile malware applicationswere obtained from ashishb [6] collections of Android malware samples.

II. INFORMATION LEAK THREATS

Benign applications. Android OS security is based on a permission model as an application is downloaded and installed. Developers of any Android application are required to define in the AndroidManifest.xml file the permissions which their application will need to run correctly. These permissions may not be required immediately. A request to grant it will made to the user if he/she uses a particular function which needs specific hardware resources. Once these permissions are granted, the application is enabled to transmit any corresponding data to relevant third parties.

TABLE I
ANDROID PERMISSION MODEL

Permissions	Details
Normal	They are expected to pose very low risk. A system will grant them automatically at the moment the application is being installed. It cannot be cancelled. E.g. SET_ALARM
Signature	These permissions are also given at the time of an installation but it should be there the compliance of the certificates E.g. READ_VOICEMAIL
Special	Special permissions actually belong to the signature permissions but they act slightly in a different way. They are extra sensitive, therefore applications would rather avoid asking for them SYSTEM_ALERT_WINDOW and WRITE_SETTINGS
Dangerous	These permissions are organized in certain groups. If one permission is granted to an application, the other permissions within that group is also granted. E.g. READ_CONTECTS and WRITE_CONTECTS

Officially these permissions are divided into 4 classes [7]. However, there are 3 protection levels. Special permissions do not have a separate protection level. The purpose of these permissions and classification of them is to protect the privacy of an Android user. If one grants the permission for an application to read or write contacts or SMS messages, a potential threat will be a misuse of the above-mentioned information when the relevant application uses it improperly.

The downside of this model is that a regular user may not always be aware of the significance of these permissions. A lack of interest of a personal security may lead to personal information being exposed to some unauthorized parties.

Android malware. After a permission is granted, there are no limitations on how the recourses of a smartphone are used [8]. Information leak in benign applications is an open question but malware can exploit it to a higher degree.

SophosLabs has collected almost 1.5 million of unique Android malware samples [9]. Their chart gives a suggestion what kind of threats Android users may expect.

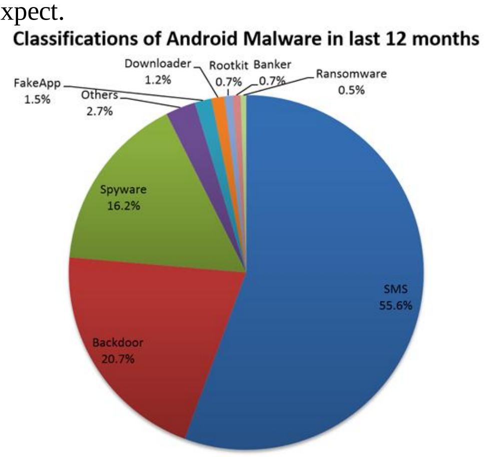


Fig. 1. SophosLabs malware statistics

The popularity of SMS malware accounts for the easiest way to attackers to profit on their malign code distribution. An extra attention should be paid while granting this permission.

Android spying applications. There is a number of officially available spying applications on Play Store or available via Google Search after submitting any relevant keywords. Some of them are heavily promoted and corresponding ads will appear during the search.

If these spying applications were used as they are officially introduced, it would rise no concerns. They are introduced as a children monitoring tool or an office smartphone control application. The reality as the research [10] shows can be different.Violent partners tend to install these applications on their victims' devices in order to track their location and communication which leads to a higher degree violence.

This research will focus on the above-mentioned types of applications. As all the security is based on the permissions in Android, Permission Management System, the prototype, has been introducedfor any potential information leak threats.

III. OVERVIEW OF THE CURRENTLY COMPLETED RESEARCHES

A huge number of researches has been completed on the AndroidOS, and a considerable number of them is dedicated to its permission model. Permissions may hardly be enough to tell if that application is malware or a benign one, but it is good enough to give a general view of what kind of information could be made available to someunauthorized parties.

Tianliang Lu and Su Hou have proposed a two-layered malware detection model [11] in order to improve the accuracy.Malware requested permissions are often similar to the permissions requested by benign applications. Sensitive permission model analysis along with the machine learning would do a better job as it is implied. Random forest is used as a machine learning algorithm for the first layer, meanwhile sensitive permission rules are used by the second layer.

The research completed by Gurol Canbek and others [12] highlights the importance of a regular Android user to understand permissions which are requested by an application instead of making statistics on the most frequently requested permissions by malware and benign applications. Their solution was to group semantically 251 Android permissions into 12 clusters. They have also proposed a visualization approach which is to look more conventional to end users and experts.

Another attempt to use permissions in order to detect any malware which leads to uncontrollable information leak is made by Abdirashid Ahmed Sahal and the others [13]. They have introduced a new weighting method which they call TF-IDFCF. They claim their detection rate is above 95.3 %. They decompile Android application files in order to read their requestable permissions which are stored in the AndroidManifest.xml file. Unique identified permissions in malware and benign applications are used to build a binary matrix. An enhanced TF-IDF method is used to select features while building their datasets. Finally, in order to detect any potentially negative application, multiple classifiers are trained.

What concerns spyware applications and a detection of them, there are also some papers available. Mustafa Hassan Saad has proposed in his paper a spyware application for a better understanding of the ways the spyware applications work and a solution to fight any spyware which is called DroidSmartFuzzer [14].

It is stated in the abovementioned research that spyware is a concern for privacy as it can overtake SMS messages, incoming and outgoing calls, andit transmits data via internet.DroidSmartFuzzer is based on a Fuzz testing which is an effective technique to find any security vulnerabilities. The software gets an input of a big amount of diverse data, and it is being monitored during this process for any unusual behavior, crashes and fails. A specific goal of DroidSmartFuzzer in that particular case was to spot any internet usage by some unauthorized applications using the following permissions:

- RECEIVE_SMS
- PROCESS_OUTGOING_CALLS
- READ_PHONE_STATE

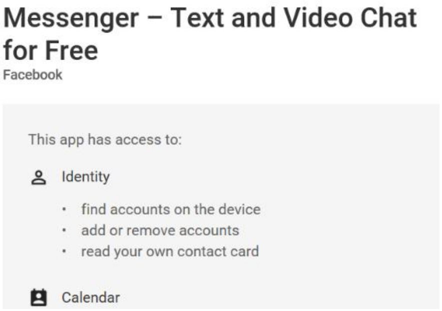
As the test was completed, it has confirmed that according to the authors their application was successful to report any spying activity.

IV. ANALYSES OF THE CURRENTLY AVAILABLE ANDROID INFORMATION LEAK MONITORING TOOLS

Since Android permission model is so important for users' sensitive information, relevant attention should be paid to any existing tools. Developers define in the manifest file which permissions are needed for that application. A user can either grant it or not but not granting may lead to an improper functioning.

A. *Android Play Store permission review section*

Android Play Store is the very first place where a user can review these permissions in order to assess any sensitive information leak.However, getting an access to this section might be slightly complicated at first. One has to pick the required applications, click on the title READ MORE, scroll to the bottom of the pop-up window, and click "View Details"underthe "Permissions" title.



Messenger – Text and Video Chat for Free
Facebook

This app has access to:

Identity
- find accounts on the device
- add or remove accounts
- read your own contact card

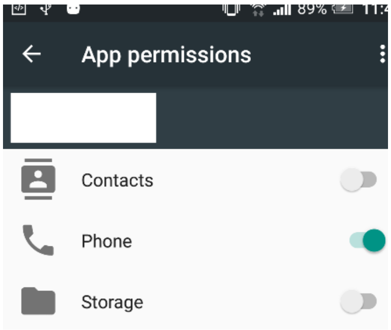
Calendar

Fig. 2. A part of Messenger permissions

B. *Permission monitoring via settings*

It was not possible to toggle any granted permissions before Android 6.0 "Marshmallow" has been released in 2015 [15]. Usually that option is available via Settings > Apps / Application Manager > Permissions. It may differ however due to a manufacturer.

A screenshot is provided below. Dangerous permission groups can be granted or revoked by using a toggle switch. Normal permissions are granted automatically.



App permissions

Contacts ○
Phone ●
Storage ○

Fig. 3. Permission overview via settings

C. *Third party applications*

There are somethird-party applications for a permission review which gives a good idea of any potentialleak of sensitive information. To name a few of them:

- Application Inspector
- APK Analyzer
- Package Info

These applications will usually scan the device for any installed applications in order to produce a list of them. As that list is further explored, one can see after picking a particular application some more details about it. It may include the version number, installation path, update time, libraries, granted permissions and permissions to be requested as well as some other details.

APK Analyzer has a good function which allows a downloaded APK package to be scanned by that application before it is installed. It gives a chance for a permission review one more time.

A tool which gives a more focused review on permissions might be useful. A regular user might not be persistent enough to look online for further explanations on certain permissions and how that type of information will be used. A personal factor on information sensitivity value might also introduce a better understanding of any potential information leak.

V. INFORMATION LEAK MONITORING ON V-S AXES

It was decided that V-S axis method [16] is the most appropriatefor the sensitivity assessment of permissions and their associated information.One axis isfor**information value (X)**and the other one is for **permission sensitivity (Y)**.As different levels are assigned on these 2 axes, different security measures can be applied.

The levels of the axis are the following ones:

Permission**sensitivity (Y)**: low, middle, and high.

Information **value (X)**: low, middle, and high.

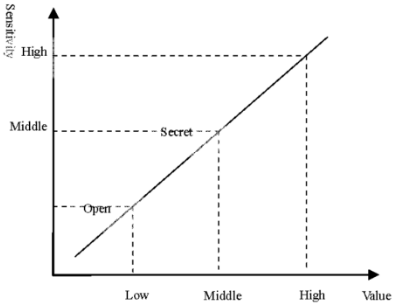


Fig. 4. V-S axes and their levels

The official Android classification of permissions [17] was used for permission sensitivity (Y). Permissions originally are classified into 4 groups: normal, dangerous, signature, and special ones. These permissions were assigned to the sensitivity axis (Y) in the following way:

TABLE II
SENSITIVITY AXIS (Y) BASED ON PERMISSIONS

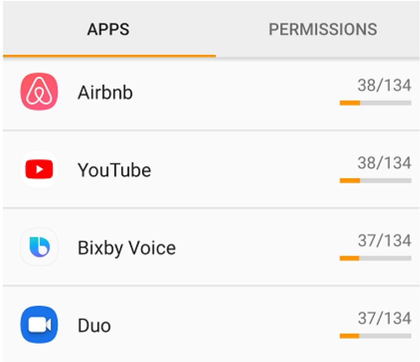
Axis (Y) level	Points	Assigned permissions
Low	0	Normal–they are not dangerous officially. Granted automatically.
Middle	1	Normal – they are not dangerous officially by may cause issues. E.g . CHANGE_NETWORK_STATE
High	2	Dangerous –dangerous permission groups. They may cause some sensitive information leak

Information value axis (X) is dedicatedto a personal assessment of the stored information. The prototype uses the default levels for this axis, but they are available for adjustingat any time.

TABLE III
VALUE AXIS (X) BASED ON PERSONAL VIEW

Axis (X) level	Points	Information value
Low	0	Low value information. A user is not concerned to lose it. Low sensitivity (Y) is matched with low value (X) by default.
Middle	1	Average value information. A user may regret to lose it. Middle sensitivity (Y) is matched with middle value (X) by default.
High	2	High value information. A user does not want to lose it. High sensitivity (Y) is matched with high value (X) by default.

Permission Management System, the proposed prototype,is based on these two axes. As this prototype is launched, it starts scanning all the installed applications. APPS list is produced by default where applications are ranked according to their danger point score. The second list PERMISSIONS is the one where permissions are ranked by the frequency of their usage. It gives a user a quick review of any potential sensitive information leak.



Airbnb 38/134

YouTube 38/134

Bixby Voice 37/134

Duo 37/134

Fig. 5. The prototype

All the permissions from **dangerous** permission group were used for permission sensitivity (Y) axis.Dangerous permissions are assigned by default to the level **High (2)**.

TABLE IV
PERMISSION GROUPS AND MAX. POINT SCORE

Permission group	Permissions and max. score on both axis			
	Permissions	*Y*	*X*	*Y * X*
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
…	…	…	…	…
Maximum point score for dangerous permissions				104

Some normal permissions were picked for using themwith the permission sensitivity (Y) axis.The default value isset to**Middle (1)**. It is set to High (2) when maximum point score is calculated which equals 134.Normal permissions are considered to be not dangerous and they are granted automatically as an application is getting installed, but they may cause some inconvenience. Besides some normal permissions like CHANGE_WIFI_STATE are very common among malware applications.

TABLE V
MAX. SCORE FOR POTENTIALLY DANGEROUS

Permissions	Y	X	Y * X
CHANGE_NETWORK_STATE	1	2	2
CHANGE_WIFI_STATE	1	2	2
MODIFY_AUDIO_SETTINGS	1	2	2
REQUEST_DELETE_PACKAG ES	1	2	2
NFC	1	2	2
REORDER_TASKS	1	2	2
REQUEST_INSTALL_PACKAG ES	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 dangerous permissions			30

The maximum danger point score is 104 + 30 = 134. Default levels are used for the information value (X) axis but a user can change it. As the tables above suggest, the default information value (X) axis has the level High (2) when it is matched with dangerous permissions the axis Y. The default level on the information value (X) axis is Middle (1) when it is matched with some picked normal permissions on the axis Y. If the level Low (0) is chosen, it will be multiplied by 0 which renders that permission unconsidered.

VI. EXPERIMENTAL FINDINGS

This experiment has been completed with the following purposes:

1) Do commercial spyware and malware have on average a higher score over benign applications?

2) Which permissions are the most common for benign, malware and spyware applications?

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

The test includes 100 benign applications, 41 malware and 28 commercial spyware applications.

Benign applications were downloaded from Play Storeusing 5 categories: shopping, finance, communication, education and business. These categories were selected randomly. Top 20 applications were selected from each of these 5 categories.

Malware applications were downloaded from GitHub [6]. Meanwhile commercial spyware applications were randomly downloaded from Play Store or from their original distributors.

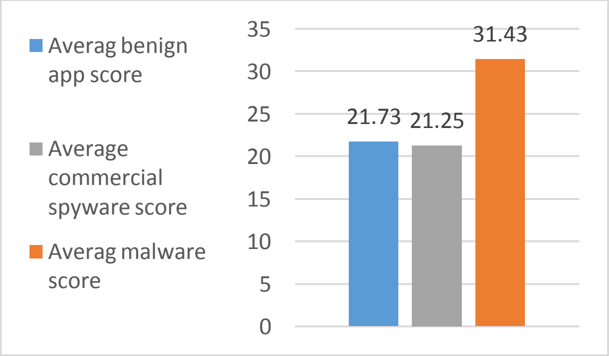


Fig. 6. Average danger point score

As one can see in the chart, malware applications have on average a higher danger point score by 1/3.The paper [18] claims that malware applications usually tend to request more permissions than benign ones. That could be the case.

Permissions solely may not however reflect the whole danger of malware due to its uncontrollable information leak.A malware application may ask just a few permissions to look completely safe but if it includes e.g. SEND_SMS, it can send SMS messages to bring a high financial loss. Permissions may not reflect the danger of spying either. If e.g. a physical attack follows spying, it is more than an information leak.

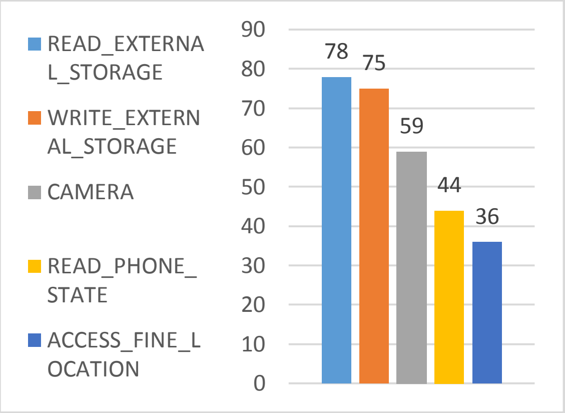


Fig. 7. The most frequent benign application permissions

Benign applications are mostly eager to use the external storage of a device.They would also need access to a camera or location.

Malware would tend to use a different set of applications as it was noticed in the paper [18].More attention was paid to dangerous ones in this case due to more sensitive nature.

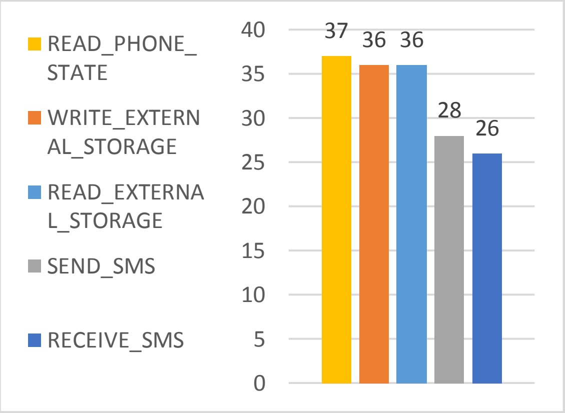


Fig. 8. The most frequent malware permissions

READ_PHONE_STATE dominates but an access to the external storage is also very important. Permissions for SMS messages are common.

Commercial spying applications will most frequently ask for the location of the device. Except reading the storage and the phone state, they will also need the contacts. The set of permissions will mainly depend of the functionality.

No scan of permissions may work if the device in enabled for such default services like Find My Mobile (Samsung). It is meant to find the lost device but it could be used to spy on close people to some extentwhen these devices are registered on the same account. Tracking services as for the lost phoneare available at https://findmymobile.samsung.com.

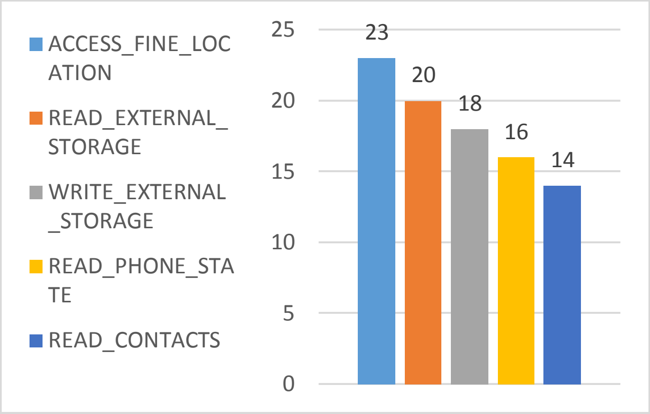


Fig. 9. The most frequent commercial spyware permissions

Further work can be done to assign a higher point score for the most common malware or commercial spyware permission sets which would allow to identify it easier. It would also suggest to double check a corresponding application with an anti-virus tool or just remove it.

VII. Conclusions

Android OS uses permission protection levels. These permissions are not always explanatory enough to understand their importance. Granting a permission keeps one informed that this type of information is used but there are no methods to reveal how it is used.

The prototype provides a quick and user-friendly assessment of a potential sensitive information leak. The danger of an information leak may not always be reflected with permissions if any further information misuse is involved for a physical attack or violence.

The research includes 100 benign applications, 41 malware and 28 commercial spyware applications.They seem to have their typical set of permissions. A further study of these sets may lead to increased safety capabilities.

REFERENCES

[1] (2019) Deuthche Welle, “Smartphones: Live longer, be greener”. [Online]. Available at:https://www.dw.com/en/smartphones-live-longer-be-greener/a-46423527.

[2] Q. Chen, J. Wang and Y. Wang, "An Online Approach for Detecting Repackaged Android Applications Based on Multi-user Collaboration," 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), Beijing, 2015, pp. 312-315.Available at: https://ieeexplore.ieee.org/abstract/document/7518244

[3] Kaspersky Lab DAILY, “Google Trades Privacy and Security for Hangouts”. Available at https://www.kaspersky.com/blog/google-privacy-hangouts/1993/

[4] Spyzie, “All-Inclusive Phone Spy”. Available at https://www.spyzie.com/ad/phone-spy-amp.html?gclid=EAIaIQobChMI9u3YsvO-4QIVV-d3Ch08ggReEAAYASAAEgKg3_D_BwE

[5] R. Chatterjee et al., "The Spyware Used in Intimate Partner Violence," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 2018, pp. 441-458. Available at: https://ieeexplore.ieee.org/document/8418618

[6] GitHub, Inc., "Ashishb Collection of Android Malware Samples".Available at: https://github.com/ashishb/android-malware

[7] Permissions Overview, 2019. Available at: https://developer.android.com/guide/topics/permissions/overview#normal-dangerous

[8] O. S. J. Nisha and S. M. S. Bhanu, "Detection of repackaged Android applications based on Apps Permissions," 2018 4th International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, 2018, pp. 1-8. Available at: https://ieeexplore.ieee.org/document/8388984

[9] Rowland Yu & William Lee, "VB2015 paper: Will Android Trojans, Worms or Rootkits Survive in SEAndroid and Containerization?", Sophos, Australia. Available at: https://www.virusbulletin.com/virusbulletin/2016/02/vb2015-paper-will-android-trojans-worms-or-rootkits-survive-seandroid-and-containerization/

[10] R. Chatterjee et al., "The Spyware Used in Intimate Partner Violence," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 2018, pp. 441-458. Available at: https://ieeexplore.ieee.org/document/8418618

[11] X. Liu and J. Liu, "A Two-Layered Permission-Based Android Malware Detection Scheme," 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, Oxford, 2014, pp. 142-148. Available at: https://ieeexplore.ieee.org/document/6834956

[12] G. Canbek, N. Baykal and S. Sagiroglu, "Clustering and visualization of mobile application permissions for end users and malware analysts," 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, 2017, pp. 1-10. Available at: https://ieeexplore.ieee.org/document/7916512

[13] A. Sahal, S. Alam and I. Soğukpinar, "Mining and Detection of Android Malware Based on Permissions," 2018 3rd International Conference on Computer Science and Engineering (UBMK), Sarajevo, 2018, pp. 264-268. Available at: https://ieeexplore.ieee.org/document/8566510

[14] M. H. Saad, A. Serageldin and G. I. Salama, "Android spyware disease and medication," 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), Cape Town, 2015, pp. 118-125. Available at: https://ieeexplore.ieee.org/document/7435516

[15] 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

[16] X. Shi, D. Li, H. Zhu and W. Zhang, "Research on Supply Chain Information Classification Based on Information Value and Information Sensitivity," 2007 International Conference on Service Systems and Service Management, Chengdu, 2007, pp. 1-7. Available at: http://ieeexplore.ieee.org/document/4280248/

[17] "Protection levels". Available at: https://developer.android.com/guide/topics/permissions/overview#normal-dangerous

[18] P. Xiong, X. Wang, W. Niu, T. Zhu and G. Li, "Android malware detection with contrasting permission patterns," in China Communications, vol. 11, no. 8, pp. 1-14, Aug. 2014. Available at: https://ieeexplore.ieee.org/document/6911083