International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 32 العدد
April 2023 ابريل
المجلة الدولية للعلوم والتقنية
ISTJ

Dangerous Permissions in Android: a preliminary study on malware risks based on user feedback and market longevity

Sumia Abdussalam Elagtel[1], Mabruka Khlifa Karkeb[2], Waled Milad Alashheb[3]

1,2. The higher Institute of Science and Technology- Souq Aljuma
3.The higher Institute of Science and Technology- Tripoli
mabruka.karkeb@gmail.com

الملخص

نظام الإذن في أندرويد هو الآلية المركزية لأمان أندرويد التي تنظم تنفيذ مهام التطبيقات. بعض الأذونات المتاحة مصنفة كخطيرة ويجب أن ينظر إليها المطورون بعناية عند تطوير تطبيقاتهم، حيث يمكن أن تؤثر سلبًا على معدلات التثبيت ورضا المستخدم ومعدلات إلغاء التثبيت، فضلاً عن احتمالية التعرض للتصنيف من قبل برامج مكافحة الفيروسات المختلفة. بنفس الطريقة التي يتم التعرف على حجم التطبيق كعامل في معدلات تثبيت التطبيقات، نحن مهتمون بدراسة ما إذا كانت الأذونات الخطيرة في أندرويد يمكن أن تؤثر على دورة حياة التطبيق في متجر Google Play. في هذه الورقة، نقترح دراسة تجريبية أولية لـ 173 إذنًا مختلفًا على 130,000 تطبيق للحصول على رؤى حول الأذونات الخطيرة في أندرويد وعلاقتها بتصنيفات البرمجيات الخبيثة وتعليقات المستخدم والعمر الافتراضي في سوق التطبيقات.

Abstract

The Android permission system is the central Android security mechanism that regulates the execution of application tasks. Some of the available permissions are tagged as dangerous and ought to be carefully considered by developers when developing their apps, as these could affect negatively their install, user satisfaction, uninstall rates, as well as the probability of being flagged by various antiviruses. In the same way that app sizes are recognised

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

as a factor in the install rates of apps, examining if harmful Android permissions can impact an app's lifecycle in the Google Play store is something, we're interested in. In this work to present a preliminary empirical analysis of 173 distinct permissions on 130,000 apps to gain knowledge about risky Android permissions and their associations with malware flags, user reviews, and app market viability.

Keywords Android Security, Permissions, preliminary, Malware, Dangerous, feedback.

I. Introduction

According to Gartner projections, by the end of 2017, mobile applications would have been downloaded over 268 billion times, generating revenue of over $77 billion and making them one of the most popular computing tools for users around the world [4]. Such huge numbers are mostly driven by the Google Android mobile OS which has a smart phone market share of 82.8% [5], mainly because it is open source and has a large collection of applications present in the official and third-party Android app markets. A key security mechanism of Android is its permission system, which control the privileges of applications, where apps must request access to specific permissions in order to perform specific functions. This mechanism requires that app developers declare which sensitive resources will be used by their applications. The users have to agree with the requests when installing/using the applications. This constrains a given application to the resources it can request during runtime. Android itself defines several categories of permissions, among which ”dangerous” ones, deemed more critical and privacy sensitive. Although there are guidelines for the use of these permissions, it is ultimately up to app developers to decide whether to ask or not for permissions for a given app. This is not always a trivial ordeal. In particular, given the update policy of Android apps from the Google Play Store which allow apps to be automatically updated when the new version is not asking for new permissions, a developer may consider asking right away for permissions needed

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

for future functionalities of her app. There are reasons to believe dangerous permissions may affect an app's success: i) mainly users may be discouraged from installing an app asking for too many dangerous permissions, ii) users may get annoyed when apps ask for those permissions at run time, iii) these apps may get flagged, possibly unduly, by anti-viruses, iv) users may thus be incentivised to give negative feedback about these apps and eventually uninstall them.

In short, while it is common knowledge to app developers that the size of their app can affect its success, there is a shortage of studies investigating the impact of dangerous permissions.

This paper investigates the use of more than 170 permissions for 130,000 apps on the Android Market. At first look at the permission use for different categories of apps and for free vs. paid apps. Then it focuses on two popular categories, Tools and Communication, with respectively 1735 and 1992 applications. The paper investigated the malware risk posed by these applications and found, unsurprisingly, that malicious applications require significantly more dangerous permissions than safe ones. Less obvious is the fact that the rating score of an application could be an indicator of malware risk. The rest of this paper is organized as follows:

In Section 2, there was a brief background. Section 3 presents related work. The data collection process detailed and the objectives of the study in Section 4. Empirical study presented in Section 5. Finally, Section 6 conclusions and suggests future work.

II. Background

In a pessimistic scenario, all Android applications are considered to be potentially buggy or malicious, each one running in a process with a low-privilege user ID and being able to only access their own files by default. If a given application requires resources or information outside of its sandbox, then it must explicitly request permission to do so. Depending on the type of

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

permission requested, the system may grant it automatically or ask the user to grant the permission. Android's permissions are classified in four levels of protection, namely Normal (lower-risk permission that gives requesting applications access to isolated application level features), Dangerous (higher-risk permission that would give a requesting application access to private user data or control over the device), Signature (permission that the system grants only if the requesting application is signed with the same certificate as the application that declared the permission), and Signature Or System (permission that the system grants only to applications that are in the Android system image or that are signed with the same certificate as the application that declared the permission). Permissions are enforced by Android at runtime but must be accepted by the user at install time. When users install a new application in Android (regardless of how the application was obtained), they are prompted to accept or deny the permissions requested by the application. On devices running Android 5.1 or lower, application permissions are either all required or all refused: users have no choice. They can either accept all permissions or refuse the application altogether, and in the latter case, they cannot use the application at all because they did not agree with certain permissions. Starting from the version 6.0 of Android, users are now able to grant permissions at run time and are no longer required to grant permissions during the initial installation of an application. In fact, the 6.0 update has provided users with improved functionality and control over their applications, giving them the possibility to revoke app permissions one by one and at anytime, via the applications settings interface. For instance, a user might choose to grant a given transport application access to their devices location while rejecting access to their contact list or SMS services.

Related work

The permission system has attracted considerable research interests and several studies were conducted to investigate the way permissions are used in Android apps, and if they could help to

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

identify malware apps. In [2], Felt et al. conducted a survey of a selection of 100 paid apps and 856 free apps taken from the Android Market. They identified the most requested permissions and observed that both free and paid apps make requests for at least one dangerous permission. They created a tool that is able to detect whether an app requests more permissions than necessary, and they observed that one third of the examined applications were over-privileged. In [1], Barrera et al. did a survey of the 1100 most popular applications downloaded in the year 2009. They found that, among the defined permissions, only a small portion is actively used by developers. In [9], Wei et al. analyzed the permission evolution in the Android ecosystem. They observed that dangerous permissions always outnumber other permission types in all versions of the Android platform. The mainstream approach for enhancing the Android permission mechanism is to identify over-declared permissions requested by an app and recommend reasonable permissions for any app [13]. In [6], Krutz et al. also studied the permission evolution in Android apps. They observed that more experimented developers are more likely to make permission-based changes, and that permissions are typically added earlier in apps commit lifetime, but their removal is more sustained throughout the commit lifetime. In [3], Frank et al. made a selection of 188,389 applications from the official Android market and studied the different combinations of permission requested by these applications. The authors identified more than 30 common patterns of permission requests and found that low reputation applications often diverge from the permission request pattern observed for high reputation applications. Another research has focused on defining risk signal to identify malware applications. In [8], Sarma et al. suggested a set of risk signals by analyzing the permission patterns in apps taken from the Android Market and within a dataset of 121 malicious apps. Finally, in [10], Zhou et al. proposed a system for detecting malicious applications in official and alternative Android markets. In [12], examined methods and tools for detecting malware with regard to their

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

methodology, accompanying datasets, and evaluation criteria. Its focus was on the ideas and risks connected to malware. Also focusing on the dangers posed by malware that targets mobile devices, and taking into account the methodology, accompanying datasets, and evaluation techniques for studies in the field of mobile malware published since 2010.In [14] was focused on examining the predictive analysis of security risks using machine learning. And conduct a comprehensive reviewed of the leading studies accomplished on investigating the vulnerabilities of the applications for the Android mobile platform. The [14] examines various well-known vulnerabilities prediction models and highlights the sources of the vulnerabilities, prediction technique, applications and the performance of these models. Some models and frameworks prove to be promising however there is still much more research needed to be done regarding security for Android applications.

In the present work, we take a somewhat different approach and consider a developer's perspective looking for insights on the impact of dangerous permissions on their app's success. A few studies such as [11] have explored factors of success for an app and come up with some insights, notably about app size, promotional images and target SDKs. To the best knowledge, there are no recent studies on the impact of permissions, in particular dangerous ones, on an app's success.

IV. Empirical study

Our research aims to better understand how permissions—especially risky ones—affect the success of Android apps. six research questions are presented here:

RQ1: Are there differences in dangerous permissions as age depending on the application categories?

RQ2: Are there differences in dangerous permissions usage depending on the application prices?

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

RQ3: Does the presence of dangerous permissions in an app affect its users' ratings also does the perceived quality reflects the malware-risk?

RQ4. Is there a difference in the use of dangerous permissions between malware and safe applications?

RQ5. Is there a difference in the use of dangerous permissions between lasting and ephemeral applications in Google Play Store?

RQ6. Is there a relationship between application malware risk and their sustainability?

In order to answer these questions, this study started from an existing dataset [3] crawled from Google Play store in 2011, and labelled the data with respect to the danger of the required permission and with respect to the harmfulness risk of the application. The hypothesis for collecting the dataset started from existing dataset [3]. There are many apps notice that name in [3] no exist in Google play store for some reason, also used those removed apps, and for the apps that still exist in Google play store, it relies on the most download apps for different categories.

For the study of permission use, the dataset cleaned up to only keep applications that have been evaluated by end users, and that declared the use of permission, ending with a total of 138,610 applications using 173 different permissions. It labelled the permission list to distinguish between Dangerous, Normal and Signature permission according to the protection level announced in the Android documentation. Also, different tags used to distinguish between permissions giving access to hardware and the ones giving access to user information. In order to investigate the difference in terms of permission use between different categories of applications, then four categories selected: Weather, Tools, Communication, and Finance. The study took a sample in each category to end up with respectively 805, 1735, 1992, 2798 applications. For the study of application harmfulness risk, it only used applications from the categories Tools and Communication,

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

given that the labelling process was challenging and time-consuming. It required identifying and locating apps that are no longer available in the Play store. On top of existing tools built to develop an API for downloading Android applications from Google Play, and considered apps that could not download, even though they were free, as being ephemeral (removed from the store). The responsibility of locating took and downloading the applications that were removed from the Play Store, in unofficial process resulted in a sample of 1833 APK files for ephemeral applications, and 1894 for those that still exist. As a second indicator of application harmfulness, the malware risk consider score defined in Equation 1. To compute this score used the online virus scan engine VirusTotal5 (https://developers.virustotal.com/). This tool is a free service that aggregates different antivirus products and analyzes files and URLs submitted by its users to check for viruses, worms, Trojans and other types of harmful content. Each submitted file is scanned by different antivirus software and products to detect whether the application is malicious or not. At the time of the experiment, VirusTotal had used 63 antivirus products and online blacklisting services. These services allowed us to label 2221 malware applications over the total 3727 analyzed apps.

$$\text{Malware\_risk (App)} = \frac{\text{Nb Antivirus detected App as Malware}}{\text{Nb Used Antivirus}} \qquad (1)$$

In the remainder of this section, the research method presents to address each question, and the obtained results. All the material used to run experiments is publicly available in a comprehensive replication package [7].

A. Permission Use

RQ1: Are there differences in dangerous permissions as age depending on the application categories? As shown in Table 1, there are variations in terms of permission use, especially dangerous ones. On average, communication apps use more

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

dangerous permissions (4.32) than the other categories (1.79, 2.99, and 2.12).

TABLE 1. Descriptive statistics of the permission use in four applications

Category	Permissions	Dangerous	Normal	Signature
Communication	Min	0	0	0
	Max	49	20	41
	Avg	4.15	2.38	0.22
	SD	4.15	1.9	1.08
Finance	Min	0	0	0
	Max	13	12	3
	Avg	1.79	1.77	0.04
	SD	1.97	1.09	0.25
Tools	Min	0	0	0
	Max	20	14	7
	Avg	2.24	1.96	0.15
	SD	2.99	1.59	0.58
Weather	Min	0	0	0
	Max	11	5	3
	Avg	2.12	2.51	0.02
	SD	1.97	1.39	0.15

This can be explained by the fact that many of the permissions considered as dangerous are related to communication and are needed in the apps (e.g., Full_Internet_Access, Access_Network State, View Wi Fi State, and Send SMS Messages). Also, notice that there are large variations within the categories, as evidenced by the high standard deviations.

RQ2: Are there differences in dangerous permissions usage depending on the application prices? Another general belief is that free apps can be used to disseminate spywares/malwares. To this end, they may ask for dangerous permissions. All the apps looked

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

in the four categories and compared paid and free ones. Table 2 shows that free applications use more permission (all kinds) than the paid ones. Here again, large variations observe within free and paid apps (with standard deviations larger than the means).

TABLE 2. Descriptive statistics of the permission use in free and paid applications

Category	Free				Paid			
Perm.	Min	Max	Avg	SD	Min	Max	Avg	SD
Danger.	0	49	2.71	3.20	0	17	1.58	1.96
Normal	0	20	2.10	1.54	0	12	1.64	1.26
Signature	0	41	0.12	0.68	0	5	0.04	0.31

B. User Satisfaction Analysis

In this study focus on the relation between the user satisfaction through the perceived quality, on one side, and the application harmfulness reflected by the malware-risk and application sustainability, on the other side. It measures the perceived quality of an application by the average rating score given by end users to a given application.

RQ3. Does the perceived quality reflect the malware-risk? For this research question, the average rating score of an application investigate whether is as a risk indicator. The study measures the risk of an application based on the metric defined in the previous section. In order to answer this question, two groups of applications create a low-risk application group (risk score = 0) and a high-risk application group (risk score > 0). As the data was not normally distributed, a Mann-Whitney U-Test performed to compare the variance of the average rating between the two groups. The Malware detected variable represents grouping criterion. This is a binary variable for which the study assigned 0 for low-risk applications (risk score = 0) and 1 for high-risk

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

applications. Table 3 (a) and Table 4 (a) show the results, respectively, for the Communication and Tools categories. For both categories, low-risk applications have, on average, a higher rating score than high-risk applications. The difference between the two are not, however, high enough to conclude that apps with low average rating are more likely to be malicious. Moreover, the difference was statistically significant for the Tools category, but not in the case of the Communication category.

TABLE 3. Rating difference in communication category for (a) malware vs benign apps and (b) lasting vs ephemeral apps

(a) Rating vs Risk				(b) Rating vs Sustainability			
Malw.	Benign	Z	Sig.	Last	Ephem	Z	Sig.
3.91	3.97	-1.794	0.07	3.99	3.88	-3.608	<0.001

TABLE 4. Rating difference in tools category for (a) malware vs benign apps and (b) lasting vs ephemeral apps

(a) Rating vs Risk				(b) Rating vs Sustainability			
Malw.	Benign	Z	Sig.	Last.	Ephem.	Z	Sig.
3.94	4.06	-2.795	0.005	4.06	3.92	-3.602	<0.001

C. Use of Dangerous Permissions Analysis

This part of the study analyzed the relation between the number of dangerous permissions declared by applications and its potential harmfulness (RQ4: malware risk and RQ5: sustainability). RQ4. Is there a difference in the use of dangerous permissions between malware and safe applications? To answer this question, a Mann-Whitney U Test applied to compare the degree of use of dangerous permissions between low-risk applications (risk score = 0) and high-risk applications (risk score ¿ 0). Table 5 (a) and Table 6 (a) show the results for the Communication and Tools categories,

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

respectively. There is a difference in means shown between low-risk and high-risk applications. High risk applications require, on average, slightly more dangerous permissions than low-risk ones. The difference is higher and statistically significant for the Tools category. This was not the case for the Communication category.

RQ5. Is there a difference in the use of dangerous permissions between lasting and ephemeral applications in Google Play Store? To answer this question, the degree of use of dangerous permissions compared between the lasting apps in the Google Play Store and the ephemeral ones. Then performed a Mann-Whitney U-test. And obtained the results presented in Table 5 (b) and Table 6 (b) and they are similar to those of harmfulness, i.e., small differences for both categories and statistical significance only for the Tools category.

TABLE 5. Dangerous permission difference in communication category for (a) malware vs safe apps and (b) lasting vs ephemeral apps

(a) Permissions vs Risk				(b) Permissions vs Sustainability			
Malw.	**Benign**	**Z**	**Sig.**	**Last.**	**Ephem.**	**Z**	**Sig.**
4.48	**4.07**	**-1.613**	**0.10**	**4.11**	**4.53**	**-1.511**	**0.13**

TABLE 6. Dangerous permission difference in tools category for (a) malware vs benign apps and (b) lasting vs ephemeral apps

(a) Permissions vs Risk				(b) Permissions vs Sustainability			
Malw.	**Benign**	**Z**	**Sig.**	**Last.**	**Ephem.**	**Z**	**Sig.**
2.62	**1.69**	**-5.138**	**<0.001**	**1.85**	**2.65**	**-4.362**	**<0.001**

D. Malware-Risk and Sustainability Analysis

The malware-risk score in relation to sustainability is the final topic we looked at. In order to do this, we came up with the

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

following research question: RQ6. Is there a relationship between application malware risk and their sustainability? To answer this research question, in Mann-Whitney U-Test results, which are shown in Tables 7 and 8, demonstrate that there is a substantial mean difference between the applications that are still available in the store and the applications that are no longer available for both the Communication and Tools categories. In fact, applications that were deleted from the store have a far higher malware risk score. This explains why these applications were taken down.

TABLE 7. Malware difference in communication category for lasting vs ephemeral apps

Last.	Ephem.	Z	Sig.
1.05	14.83	-36.16	<0.001

TABLE 8. Malware difference in tools category for lasting vs ephemeral apps

Last.	Ephem.	Z	Sig.
2.94	11.33	-23.84	<0.001

V. Conclusions

The essay provides with a sizable sample of both harmful and safe applications, it looked at how Android permissions were used which discovered a connection between the misuse of risky permissions and adverse application risk. To help Android developers and consumers appropriately deal with the Android permission system, the opinion, more study should be done to gain a deeper understanding of this interaction.

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

References

[1] D. Barrera, H Gne Kayacik, Paul C van Oorschot, and Anil Somayaji. 2010. A methodology for empirical analysis of permission-based security models and its application to android. In Proc. of the 17th ACM conf. on Computer and communications security. ACM, 7384.

[2] Adrienne Porter Felt, Kate Greenwood, and DavidWagner. 2011. The effectiveness of application permissions. In Proceedings of the 2nd USENIX conference on Web application development. 77.

[3] Mario Frank, Ben Dong, Adrienne Porter Felt, and Dawn Song. 2012. Mining permission request patterns from android and Facebook applications. In Data Mining (ICDM), 2012 IEEE 12th International Conference on. IEEE, 870875.

[4] Mobile Users Will Provide Personalized Data Streams to More Than 100 Apps Gartner Says by 2017 and Services Every Day. Available on line at:. [n. d.]. ([n. d.]).http://www.gartner.com/newsroom/id/2654115

[5] Smartphone OS Market Share. Available on line at: IDC. [n. d.]. ([n. d.]). http: //www.idc.com/promo/smartphone-market-share/os.

[6] Mkaouer. 2017. Who added that permission to my app?: an analysis of developer permission changes in open source Android apps. In Proc. of the 4th ICMSES. IEEE Press, 165169.

[7] Replication package:. [n. d.]. ([n. d.]). http://www-etud.iro.umontreal.ca/ saiedmoh/MobileSoftRP/index.html.

[8] Bhaskar Pratim Sarma, Ninghui Li, Chris Gates, Rahul Potharaju, Cristina Nita-Rotaru, and Ian Molloy. 2012. Android permissions: a perspective combining risks and benefits. In Proc. of the 17th ACM symposium on Access Control Models and Technologies. ACM, 1322.

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية

[9] Xuetao Wei, Lorenzo Gomez, Iulian Neamtiu, and Michalis Faloutsos. 2012. Permission evolution in the android ecosystem. In Proc. of the 28th Annual Computer Security Applications Conference. ACM, 3140.

[10] Yajin Zhou, Zhi Wang, Wu Zhou, and Xuxian Jiang. 2012. Hey, you, get off of my market: detecting malicious apps in official and alternative android markets. In NDSS, Vol. 25. 5052. Electron Devices, vol. ED-11, pp. 34-39

[11] Yuan Tian, Meiyappan Nagappan, David Lo, Ahmed E. Hassan. 2012. What are the characteristics of high-rated apps? A case study on free Android Applications. ICSME 2015: 301-310

[12] Alzubaidi, A. (2021). Recent advances in android mobile malware detection: a systematic literature review. IEEE Access, 9, 146318-146349.

[13] Z. Liu, X. Xia, D. Lo, J. Grundy, Automatic, highly accurate app permission recommendation, Automated Software Engineering (2019) 1–34.

[14] Abdullah, R. M., Abualkishik, A. Z., Isaacc, N. M., Alwan, A. A., & Gulzar, Y. (2022). An investigation study for risk calculation of security vulnerabilities on android applications. Indonesian Journal of Electrical Engineering and Computer Science, 25(3), 1736-1748.

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدوليةللعلوم والتقنية