Frontiers in Health Informatics www.ijmi.ir
2020; 9: 41 Open Access

Security challenges in android mHealth apps permissions: A case study of Persian apps

Hamid Naderi[1], Behzad Kiani[1]*

[1]Department of Medical Informatics, School of Medicine, Mashhad University of Medical Sciences, Mashhad, Iran

Article Info

Article type:
Research

Article History:
Received: 2020-06-25
Accepted: 2020-08-24
Published: 2020-09-02

**** Corresponding author:***
Behzad Kiani

Department of Medical Informatics, School of Medicine, Mashhad University of Medical Sciences, Mashhad, Iran

Email: Kianib@mums.ac.ir

Keywords:
mHealth
Mobile Application
Security
Permission
Android

A B S T R A C T

Introduction: In this study, Persian Android mobile health (mhealth) applications were studied to describe usage of dangerous permissions in health related mobile applications. So the most frequently normal and dangerous permissions used in mHealth applications were reviewed.

Material and Methods: We wrote a PHP script to crawl information of Android apps in "health" and "medicine" categories from Cafebazaar app store. Then permission information of these application were extracted.

Results: 11627 permissions from 3331 studied apps were obtained. There was at least one dangerous permission in 48% of reviewed apps. 41% of free applications, 53% of paid applications and 71% of in-purchase applications contained dangerous permissions. 1321 applications had writing permission to external storage of phone (40%), 1288 applications had access to read from external storage (39%), 422 applications could read contact list and ongoing calls (13%) and 188 applications were allowed to access phone location (5%).

Conclusion: Most of Android permissions are harmless but significant number of the apps have at least one dangerous permission which increase the security risk. So paying attention to the permissions requested in the installation step is the best way to ensure that the application installed on your phone can only access what you want.

Cite this paper as:
Naderi H, Kiani B. Security Challenges in Android mHealth Apps Permissions: A Case Study of Persian Apps. Front Health Inform. 2020; 9: 41. DOI: 10.30699/fhi.v9i1.224

INTRODUCTION

App stores that host hundreds of thousands of applications (apps) are the main distribution channel for mobile health (mHealth) apps and users can download and install third-party apps from these markets [1]. App stores have created a new software deployment ecosystem which are technically different from traditional methods [2-4]. Some third-party developers are malicious, most authors of applications are not security experts and their code may contain vulnerabilities [5].

Android is a privilege-separated operating system which additional security features are provided through permissions. Permission mechanism enforces restrictions on the specific operations that a particular process can perform. A basic Android application cannot do anything that would impact the user privacy or any data on the device, because it has no permissions associated with it by default. In the process of installing an application, the list of permissions that the app requests is shown to the user. The user should decide to accept or cancel installation. These permissions are not shown at any time after than installation step [6]. To make use of protected features of the device, one or more <uses-permission> tags must be included in the app manifest file [7]. For example, Fig 1 shows permission definition in manifest file to monitor incoming SMS messages in the app.

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.android.app.myapp" >
    <uses-permission android:name="android.permission.RECEIVE_SMS" />
    ...
</manifest>
```

Fig 1: A sample of permission definition in the app manifest file [8]

Android permissions have several protection levels. Two most important protection levels are normal and

dangerous permissions. Normal permissions do not pose much risk to the user's privacy or operation of device and the system automatically grants them. For example, permission to set the time zone is a normal permission. Dangerous permissions could potentially affect the user's privacy or the normal operation of device, therefore the system asks the user to explicitly grant those permissions in the manifest file. For example, the ability to read the user's contacts is a dangerous permission. Table 1 lists all dangerous permissions in Android according to Google [8].

Table 1: Dangerous permissions in Android apps

Permission Group	Permissions
CALENDAR	READ_CALENDAR WRITE_CALENDAR
CAMERA	CAMERA
CONTACTS	READ_CONTACTS WRITE_CONTACTS GET_ACCOUNTS
LOCATION	ACCESS_FINE_LOCATION ACCESS_COARSE_LOCATION
MICROPHONE	RECORD_AUDIO
PHONE	READ_PHONE_STATE CALL_PHONE READ_CALL_LOG WRITE_CALL_LOG ADD_VOICEMAIL USE_SIP PROCESS_OUTGOING_CALLS
SENSORS	BODY_SENSORS
SMS	SEND_SMS RECEIVE_SMS READ_SMS RECEIVE_WAP_PUSH RECEIVE_MMS
STORAGE	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE

Several studies have been done on vulnerabilities in the mobile applications but few of them have discussed Android permissions vulnerabilities. A Study by Felt et.al [9] Considered 100 paid and 856 free applications from the Android Market. Selected apps in that survey was not limited to health related topics and did not compare mobile applications based on their categories. In another study [10], requested permissions in a large number of Android applications were studied but they did not mention details of their sample and application's topic. None of these studies focused on mHealth apps permissions and vulnerabilities. In this survey, we considered only Android mHealth apps in health and medicine categories. Most of Iranian users download apps from Persian app stores. "Cafebazaar" is the largest Iranian Android app store and contained more than 3500 apps in medical and health categories in 2016 [11]. The study aims to describe security challenges of released mHealth apps permissions in Persian Android app store "Cafebazaar".

MATERIAL AND METHODS

We wrote a PHP script to crawl information of Android apps in "health" and "medicine" categories from Cafebazaar app store in August 2019. We also crawled list of permissions used in gathered apps. The information of 3390 apps were gathered in this two categories. After review information 59 apps were excluded because their scope did not relate to medicine and health. Based on the apps description we defined eight subcategories under "health" and "medicine" categories: "drug information", "traditional medicine", "fitness", "health education", "pregnancy and parturition", "diet and nutrition", "health test results" and "self-monitoring". Permissions of selected apps were overviewed and security challenges from different viewpoints were analyzed.

RESULTS

Total number of permissions used in these apps were 11627 permissions. Number of unique permissions requested in all studied apps were 365 permissions. Table 2 lists 15 top most frequently requested permissions out of 365 total different permissions in developing mHealth apps. More than 90% of total requested permissions in 3331 studied apps were permissions listed in Table 2.

Six of 15 most frequently requested permissions are dangerous. 1321 applications had writing permission to external storage of phone (40%), 1288 apps had access to read from external storage (39%), 422 apps could read contact list and ongoing calls (13%) and 188 apps requested ACCESS_COARSE_LOCATION and ACCESS_FINE_LOCATION permissions were allowed to access phone location (2%) (Table 2). Fig 2 shows comparison of top dangerous permissions used in studied apps. In this figure, the distribution of apps based on their price and purchase type (free, paid, in-purchase) is also considered. 41% of free apps, 53% of paid apps and 71% of in-purchase apps contained dangerous permissions.

Fig 3 shows number of apps grouping by number of requested dangerous permissions. There is at least one dangerous permission in 48% of reviewed apps. Our results show 6% of studied apps had more than 5 dangerous permissions. In other words, about 94% of studied apps had 1-5 dangerous permissions. Also there is an app with 13 dangerous permissions which contained the most number of dangerous permission in just one application.

Table 2: Fifteen most frequently (90%) requested permissions in developing Persian Android mHealth apps

Permission	Dangerous Permission	Number of Apps
INTERNET (Allows applications to open network sockets)	No	2489
WRITE_EXTERNAL_STORAGE (Allows an application to write to external storage)	Yes	1321
READ_EXTERNAL_STORAGE (Allows an application to read from external storage)	Yes	1288
BILLING (Allows In-app purchase)	No	1107
ACCESS_NETWORK_STATE (Allows applications to access information about networks)	No	1022
VIBRATE (Allows access to the vibrator)	No	977
WAKE_LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming)	No	693
READ_PHONE_STATE (Allows read only access to phone state, including the phone number of the device, current cellular network information, the status of any ongoing calls, and a list of any phone accounts registered on the device)	Yes	422
RECEIVE_BOOT_COMPLETED (Allows automatically run an application on phone startup)	No	308
GET_ACCOUNTS (Allows access to the list of accounts in the Accounts Service)	Yes	222
CHANGE_NETWORK_STATE	No	217
ACCESS_WIFI_STATE (Allows applications to access information about Wi-Fi networks)	No	213
ACCESS_COARSE_LOCATION (Allows an app to access approximate location)	Yes	112
GET TASKS	No	86
ACCESS_FINE_LOCATION (Allows an app to access precise location)	Yes	76

Table 3 describes usage of permissions by most active mobile health application developers. 15 developers with the highest number of published applications in the health field were selected. 362 mHealth apps were published in Cafebazaar app store by these active developers. Totally 1108 permissions were used in these apps, which 478 permissions were dangerous permissions (43%).

We defined 8 subcategories in health and medicine to compare applications based on their topic in Cafebazaar app store. We also selected top 10 most popular mHealth apps and put them in 8 predefined subcategories. As Table 4 shows, we can see distribution of dangerous permissions in these most popular mHealth apps. WRITE_EXTERNAL_STORAGE, READ_EXTERNAL_STORAGE, READ_PHONE_STATE, GET_ACCOUNTS, ACCESS_COARSE_LOCATION, ACCESS_FINE_LOCATION, CAMERA and READ_CONTACTS are dangerous permissions used in these 80 popular apps.

Total number of dangerous permissions requested in these apps is 123 with the average of 1.5 per app. Minimum and maximum number of dangerous permissions in selected popular apps has been observed in the "health test results" and "self-monitoring" subcategories respectively. Permissions to transfer data with external storage that includes WRITE_EXTERNAL_STORAGE and READ_EXTERNAL_STORAGE are the most frequent dangerous permissions in all subcategories.

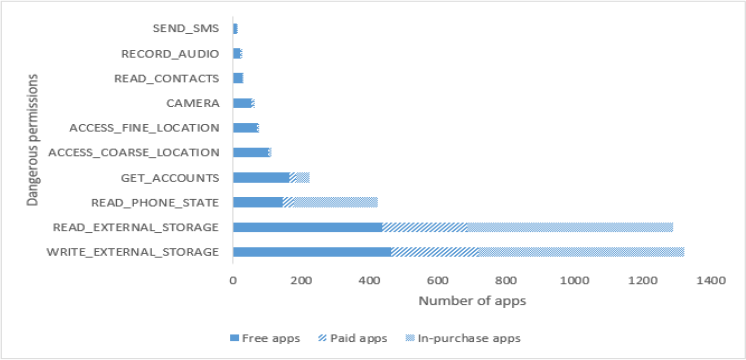

Fig 2: Comparison of different dangerous permissions used in studied apps

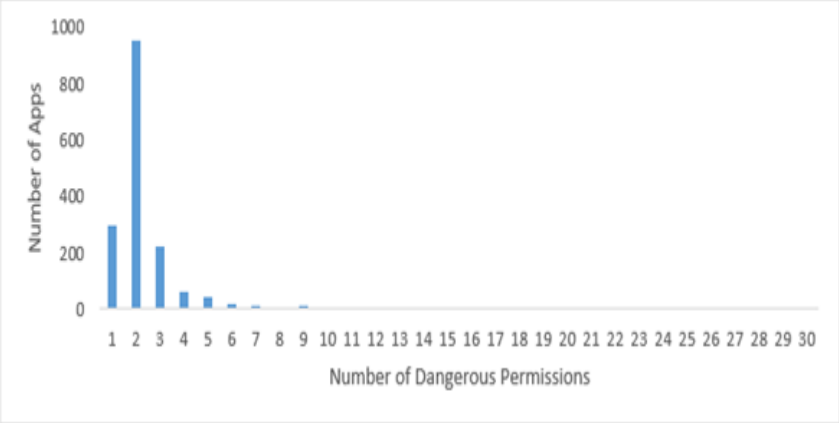

Fig 3: Number of apps group by number of dangerous permissions

Table 3: The use of permissions by most active mHealth apps developers in Cafebazaar app store

Developer	Free apps	Paid apps	In-purchase apps	Total apps	Average of permissions per app	Average of dangerous permissions per app
developer 1	0	1	31	32	4.94	2.00
developer 2	31	1	0	32	1.09	0
developer 3	0	3	28	31	1.94	1.94
developer 4	0	0	28	28	2.21	2.21
developer 5	0	5	22	27	1.63	0
developer 6	0	0	28	28	5.00	2.00
developer 7	8	1	14	23	2.52	0.65
developer 8	1	0	19	20	2.40	1.20
developer 9	0	0	23	23	5.00	2.00
developer 10	0	0	23	23	1.74	1.74
developer 11	18	2	1	21	2.81	0.81
developer 12	6	7	4	17	1.59	0.47
developer 13	0	0	18	18	5.56	2.22
developer 14	0	0	20	20	5.00	2.00
developer 15	5	13	1	19	3.26	0.32

Table 4: Dangerous permissions of most popular mHealth apps in different subcategories

Permission	Drug information	Traditional medicine	Fitness	Health education	Pregnancy and parturition	Diet and nutrition	Health test results	Self-monitoring	Sum
WRITE_EXTERNAL_STORAGE	7	2	6	7	6	3	2	6	39
READ_EXTERNAL_STORAGE	7	2	6	6	6	3	2	6	38
READ_PHONE_STATE	3	2	3	1	2	2	2	3	18
GET_ACCOUNTS	1	2	2	1	1	2	1	3	13
ACCESS_COARSE_LOCATION	0	0	1	0	1	0	0	2	4
ACCESS_FINE_LOCATION	0	1	1	0	0	0	0	3	5
CAMERA	0	1	0	0	0	0	0	3	4
READ_CONTACTS	0	0	0	0	0	0	0	2	2
Sum	18	10	19	15	16	10	7	28	123

DISCUSSION

This survey was one of the first to study security challenges of Android mHealth apps. Our study results indicate the status of dangerous permissions usage in mHealth apps which almost half of the apps have at least one dangerous permission. Although we focused on mHealth apps in this survey, the results of our study about the most frequent dangerous permissions are consistent with the results of previous studies. The order of requested dangerous permissions is almost the same. Data transmission with external storage, get phone status information, access to the location and read contacts list are ordinary the most frequent dangerous permissions in these studies [12, 13].

Unnecessary permission warnings in over privileged applications reduced user's attention to warning about apps vulnerabilities [14]. Although Android's permission system is intended to inform users about the risks of installing apps, current Android permission warnings do not help most users make good security decisions [6]. The results of a study conducted by Enck [15] showed that only 17% of participants paid attention to permissions during installation and usually Android permission warnings are ignored by users. Most surveys have found that people are very protective of their personal data when asked directly about their privacy preferences [16, 17] but their actions do not always correspond to their preferences [18, 19]. This may be because users overestimate their privacy or they do not understand what actions violate their privacy preferences.

We considered the number of dangerous permissions requested in an app as an indicator of application vulnerability. Storage group permissions are the most requested dangerous permissions in all subcategories. In many mobile applications, some of the information needs to be stored in storage, so access to external storage in these apps should be considered. For example, to store data logs in self-monitoring apps, the application should be able to write to the external storage. It requires WRITE_EXTERNAL_STORAGE permission. Also, to retrieve data stored in storage, display it in the app or report to the user, the application should have access to read stored information. To this end, READ_EXTERNAL_STORAGE permission should be defined at development time. Self-monitoring apps help users creating a healthy lifestyle. These apps let users view a complete history of their health data, including activity, sleep, weight, and monitor blood pressure, heart rate and pulse wave velocity. Users can see their trends, track progress, and improve over time. In self-monitoring apps GPS is used to help users tracking steps. The use of GPS in app requires ACCESS_COARSE_LOCATION and ACCESS_FINE_LOCATION permissions. In some apps, users can share their photos. Due to the fact that access to the camera should exist in these apps, the CAMERA permission is required. Our study results show the apps in self-monitoring subcategory have the highest levels of vulnerability.

INTERNET permission was the most common requested permission in studied apps. Most of the time, the log of health data is sent to the server as soon as phone device is connected to the Internet. Most of apps allow users to share their health information on social networks with friends and family and experience a healthy competition with each other. Also large number of mHealth apps update their content continuously. INTERNET permission is required to sync data stored on the phone with server, share information and update content of applications. In some other studies [6, 20], the INTERNET permission has been reported as the most frequent dangerous permission. Since INTERNET permission was requested by many apps so Google decided to change its protection level to normal and no longer consider INTERNET as a dangerous permission. In this study we did not consider INTERNET as a dangerous permission by itself but when Internet connection is allowed with a dangerous permission in an application simultaneously, the risk of privacy violations increase significantly.

There were some limitations in our study. In this study we just considered published applications in Cafebazaar app store as the most popular Persian Android app store. Although there are several other Persian app stores, there is a big difference between the number of released apps in Cafebazaar and other app stores. We had collected and reviewed all apps in both health and medicine categories but it is possible that a limited number of developers put their health-related apps in other categories. We did not consider these mHealth apps in our study.

CONCLUSION

There are a lot of permissions that Android developers use to make their products work well. Most of permissions are harmless but when normal permissions are used together in an application, the possibility of some threats are increased. Also, the use of some normal permissions, such as INTERNET permission, with dangerous permissions can increase the risk. So pay attention to the permissions requested in the installation step is the best way to ensure that the application installed on your phone can only access what you want.

AUTHOR'S CONTRIBUTION

The authors agree on this final form of the manuscript, and attested that all authors contributed

in the final draft of the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest regarding the publication of this study.

FINANCIAL DISCLOSURE

No financial interests related to the material of this manuscript have been declared.

REFERENCES

1. Xu W, Liu Y. mHealthApps: A repository and database of mobile health apps. JMIR Mhealth Uhealth. 2015; 3(1): e28. PMID: 25786060 DOI: 10.2196/mhealth.4026 [PubMed]
2. Harman M, Jia Y, Zhang Y. App store mining and analysis: MSR for app stores. IEEE Working Conference on Mining Software Repositories. IEEE; 2012.
3. Lim SL, Bentley PJ. Investigating app store ranking algorithms using a simulation of mobile app ecosystems. IEEE Congress on Evolutionary Computation. IEEE; 2013.
4. Minelli R, Lanza M. Software analytics for mobile applications: Insights & lessons learned. European Conference on Software Maintenance and Reengineering. IEEE; 2013.
5. He D, Naveed M, Gunter CA, Nahrstedt K. Security concerns in Android mHealth apps. AMIA Annu Symp Proc. 2014; 2014: 645-54. PMID: 25954370 [PubMed]
6. Felt AP, Ha E, Egelman S, Haney A, Chin E, Wagner D. Android permissions: User attention, comprehension, and behavior. Symposium on Usable Privacy and Security. ACM; 2012.
7. Sbîrlea D, Burke MG, Guarnieri S, Pistoia M, Sarkar V. Automatic detection of inter-application permission leaks in android applications. IBM Journal of Research and Development. 2013; 57(6): 1-20.
8. Google Developers. Android security guide [Internet]. 2012 [cited: 2 Jun 2010]. Available from: https://developer.android.com/guide/topics/security/security.html.
9. Felt AP, Greenwood K, Wagner D. The effectiveness of application permissions. USENIX conference on Web application development. WebApps; 2011.
10. Di Cerbo F, Girardello A, Michahelles F, Voronkova S. Detection of malicious applications on android OS. International Workshop on Computational Forensics. Springer; 2010.
11. Ghazi Saeedi M, Rostam Niakan Kalhori S, Nouria R, Yasini M. Persian mHealth apps: A cross sectional study based on use case classification. Stud Health Technol Inform. 2016; 228: 230-4. PMID: 27577377 [PubMed]
12. Baalous R, Poet R. How dangerous permissions are described in android apps' privacy policies? International Conference on Security of Information and Networks. ACM; 2018.
13. Wang Y, Zheng J, Sun C, Mukkamala S. Quantitative security risk assessment of android permissions and applications. IFIP Annual Conference on Data and Applications Security and Privacy. Springer; 2013.
14. Magat WA, Viscusi WK, Huber J. Consumer processing of hazard warning information. Journal of Risk and Uncertainty. 1988; 1(2): 201-32.
15. Enck W, Ongtang M, McDaniel P. On lightweight mobile phone application certification. ACM Conference on Computer and Communications Security. ACM; 2009.
16. Ackerman MS, Cranor LF, Reagle J. Privacy in e-commerce: Examining user scenarios and privacy preferences. Conference on Electronic Commerce. ACM; 1999.
17. Buchanan T, Paine C, Joinson AN, Reips UD. Development of measures of online privacy concern and protection for use on the Internet. Journal of the American Society for Information Science and Technology. 2007; 58(2): 157-65.
18. Acquisti A. Privacy in electronic commerce and the economics of immediate gratification. ACM Conference on Electronic Commerce. ACM; 2004.
19. Jensen C, Potts C, Jensen C. Privacy practices of Internet users: Self-reports versus observed behavior. International Journal of Human-Computer Studies. 2005; 63(1-2): 203-27.
20. Barrera D, Kayacik HG, Van Oorschot PC, Somayaji A. A methodology for empirical analysis of permission-based security models and its application to android. Conference on Computer and Communications Security. ACM; 2010.