Android Users Privacy Awareness Survey

https://doi.org/10.3991/ijim.v11i3.6605

Mohammed M. Alani
Khawarizmi International College
m@alani.me

Abstract—Having a share of over 80% of the smartphone market, Android has become an important mobile operating system that is used by billions of users on daily basis. With the widespread use of smartphones in general, and Android in specific, privacy concerns grow with that expansion in the user base. With the millions of applications being downloaded by users daily, it is becoming increasingly difficult to differentiate between the good and the bad in terms of security and privacy. In this paper, we present the results of a survey conducted among 4027 Android users worldwide. This survey was conducted to measure the awareness of Android users regarding their privacy. The study measures the users' interaction with the permissions required by different applications they install. The results of the survey show apparent weakness in the awareness of Android users regarding the privacy of their data.

Keywords—android, privacy, security, malware

1 Introduction

According to [1], the number of people using smartphones is over 2 billion in 2016 and this number is expected to grow to over 2.5 billion in 2019. The recent statistics presented by Gartner in [2] show that slightly over 80% of the current smartphone market is for Android operating system.

Android operating system was initially developed by a company named Android Inc. which was later bought by Google in 2005. Officially, Android operating system was introduced to the public in 2007.

Android operating system is mostly built on open source software and released under open-source license. However, the access to Google services is closed course and done using Google Play Framework. The operating system uses Google Play store as the main source of applications. Android users can easily install applications (paid or free) from Google Play Store as long as they have a valid Google Account and a working Google Play Store.

In 2013, Google Play store hosted over 1 million applications [3]. With this huge and rapid increase in the number of applications, security challenges arise rapidly as well. Since Google does not employ a strict filtering policy like the one adopted by Microsoft in testing and filtering applications before publishing them, the probability of rogue applications gets high.

In 2015, researchers found a new type of Android adware that cannot be removed [4]. The adware, a type of malware that is aimed to collect information and produce unwanted ads, auto-roots phones and installs its malicious ads applications as system application which makes it virtually impossible to uninstall. Traces of the adware were detected in over 20,000 applications that were decoded, infected, and then repackaged to look like legitimate applications from Facebook, Twitter, and other companies and distributed through application markets other than the Google Play Store.

Recently, security researchers have revealed that over 100 malicious applications were found in the Google Play Store in [5]. These applications contained malware named Android.Spy.277.origin. This malware steals over 30 different pieces of information from the phone and sends it to the attacker's remote server. This information sent to the attacker contain some sensitive items like the phone number and IMEI among others. This malware resends all of this information every time the application is run.

Also in early 2016, Google removed 13 applications from the Google Play Store because they contained traces of malware family named "Brain Test" [6]. These applications made unauthorized downloads and attempted to get root privilege to enable them to survive factory reset. These malicious applications are capable of using compromised devices to download and positively review other malicious applications in the Play store by the same authors. This helps increase the download figures in the Play Store to the point where one of these 13 applications had over 1 million downloads before removal.

2 Previous work

In 2011, [7] introduced a malware-detection scheme based on kernel-based behavior analysis. The research focused on log collection in the Linux layer and introduced a log-analysis application to detect anomalies. The log-analysis application matches activities from these logs with signatures described by regular expression to detect any malicious activity. The prototype implemented in this paper was used to evaluate activities of 230 applications and showed promising results in detection of malicious behaviors of unknown applications.

RefRanker was proposed in 2012 [8]. RiskRanker is said to be a proactive scheme to detect zero-day Android malware. The proposed system does not rely on malware signatures like classical malware detector. It relies on analyzing whether an application is exhibiting a dangerous behavior like launching a root exploit or or sending a premium SMS in the background. The analyzer then produces a short list of applications that require further analysis. The system processed 118,318 applications and reported 3,281 risky applications. Out of those risky applications, further analysis concluded the existence of 718 malware samples.

In 2012 as well, a machine learning based system for malware detection was introduced [9]. The proposed system starts by extracting a number of features using an open-source package called Androguard [10]. The extracted features are then fed into a one-class support vector machine in an offline manner. The end product would be a classifier that is capable of identifying malware. This classifier can use the processing power of a server or a cluster of servers instead of being on-device and limit the processing power to the device capabilities.

A study was conducted in 2012 that studied the permissions requested by an applications as compared to permissions requested by other applications within the same category [11]. The aim of the study was to produce alerts to user about the risks of installing applications not only based on the permissions these applications require, rather based on the permissions required by other applications that are similar in purpose and fall within the same category. The proposal used two data sets for testing; on of 158,062 Android applications from the official Google Play Store and another dataset of 121 malicious applications. Although the proposal showed effectiveness, the extensive data analysis was costly in terms of time and processing power.

A different approach was taken by [12] published in 2012. This paper introduced a static feature-based mechanism to detect Android malware, namely DroidMat. The mechanism considers the static information including permissions, deployment of components, Intent messages passing and API calls for characterizing the Android applications behavior. The proposed system applies K-means algorithm that enhances the malware modeling capability. The experiments results showed that DroidMat recall rate was better than Androguard while it takes around half the time needed by Androguard.

In 2012 as well, a study was conducted to characterize Android malware in [13]. The study collected over 1,200 malware samples that cover majority of Android malware families. The study systematically characterize malware from various aspects, including their installation methods, activation mechanisms as well as the nature of carried malicious payloads. The study also discussed the effectiveness of Android anti-virus and anti-malware software from different vendors and their capabilities of detecting different strands of malware.

A permission-based malware detection scheme was introduced in [14] in 2013. The framework proposed in this paper aims at developing a machine learning-based malware detection system on Android to detect malware applications and to enhance security and privacy of smartphone users. The proposed system focuses on monitoring permission-based features and events obtained from the applications and analyses these features by using machine learning classifiers to classify whether the application is malicious or not.

Another framework employing machine learning was introduced in 2013 [15]. This paper evaluates a number of existing classifiers that use machine learning, using a dataset containing thousands of real applications. The paper presented a framework, named STREAM, that was developed to enable rapid large-scale validation of mobile malware machine learning classifiers.

In 2015, [16] introduced a multi-level malware detection mechanism using diverse data sources. The proposal focused on providing high speed detection with a balance between the accuracy of detection and usage of less intensive computations. The proposed method showed good detection capabilities with faster detection as compared to other detection mechanisms.

Another study focused on the effectiveness of Android Anti-virus software was published in 2016 [17]. The study performed a large scale experiment on 57 Android AVs using 2000 malware variants to evaluate whether the detection logic can be found and whether the Anti-virus software can detect the malware. These experiments showed that a majority of Anti-Virus software detects malware using simple static features. Such features can be easily obfuscated by renaming or encrypting strings and data, which can make it easy to evade detection.

3 Privacy Awareness Survey

The survey was designed to measure the awareness of users about the permissions the applications they install require. It also measure how concerned the users are with privacy and what do they consider most private data asset. The survey was designed with simple language that is easy to understand.

The survey was done using an open-source survey software named LimeSurvey [18]. The survey was open for 2-months. We used social media like Facebook, Twitter, and LinkedIn to expand the user-base reach to the survey.

A summary of the questions asked in the survey can be found in the following list:

1. Which version of Android are you using on your device?
2. Is your device rooted?
3. (If your device is rooted) Do you know exactly how many apps on your device have root access?
4. How many apps are installed on your device?
5. What is the type of data you consider most private?
6. Do you know exactly how many apps on your device have access to your most private data?
7. How often do you read the required app permissions before installing the app?
8. Have you ever refused to install an app you want because of the permissions the app requested?
9. Do you use additional tools to control privacy of your data like AppOps, Permission Control,..etc?
10. Which of the following apps are installed on your device?
    (a) Facebook Messenger
    (b) Facebook Page Manager
    (c) Viber
    (d) Whatsapp
    (e) Super-bright LED Flashlight
    (f) Google Chrome Browser
    (g) Swiftkey Keyboard
11. Are you currently using (or have previously used) antivirus or anti-malware apps on you device?
12. How many times your device have been infected with a virus or malware?
13. Have you ever installed apps from outside of Play Store?

4 Survey Results

In total, there were 4126 responses to the survey, out of which only 4027 were complete. All the results shown hereafter are for complete responses only. 34.49% of the responses came from the United States, 32.58% of the responses were from the United Arab Emirates, and the remaining 32.93% came from 29 other countries.

In Figure 1, and Table 1 you can see the responses to the first question about the Android version.

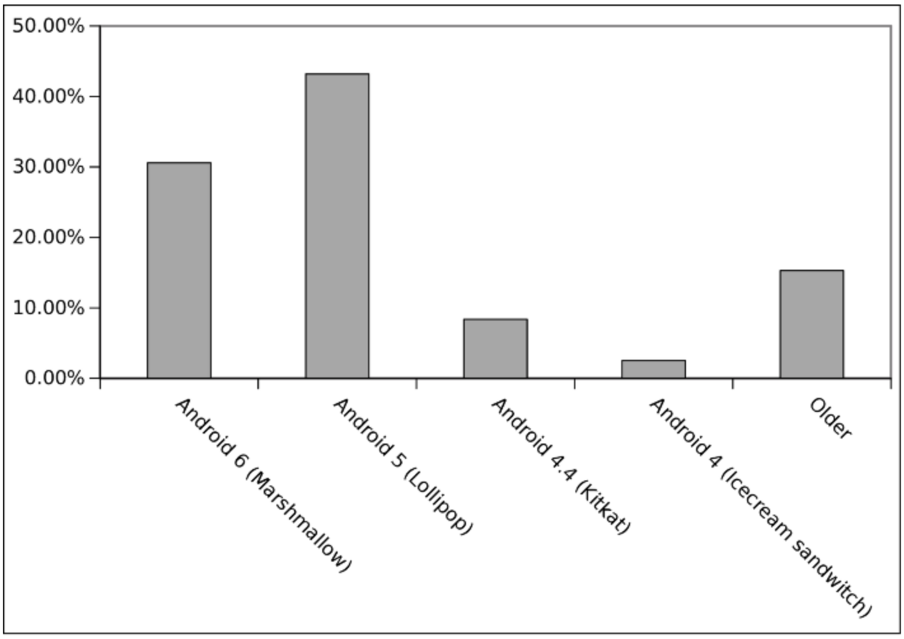

Fig. 1. Android versions for all survey responses

Table 1. Android Versions of Survey Respondents

Android Version	Number of Responses	Percentage
6 (Marshmallow)	1232	30.59%
5 (Lollipop)	1739	43.18%
4.4 (Kitkat)	338	8.39%
4 (Icecream sandwitch)	102	2.53%
Older	616	15.30%

Table 1 shows that most survey respondents were using Android 5 (Lollipop) with 43.18%. Users of Android 6 (Marshmallow) came in second with 30.59%. Android 6 came with more user-control over permissions with the ability to switch-off certain permissions for certain applications.

In response to the second question, 2190 (54.38%) respondents said that their devices are rooted. Out of those, only 1118 (51.05%) say that they know exactly how many applications in their devices have root access. This leaves 1072 (48.95%) with rooted devices and do not know exactly how many applications on their device have root access, while 1837 (45.62%) use non-rooted devices.

Table 2 and Figure 2 show the responses to the fourth question about the number of applications the respondents have installed on their devices. These results show that 74.35% of respondents have 50 applications or less installed on their devices. While only 4.30% have 51-75 applications installed, 9.93% have 75-100 applications installed. Only 11.42% respondents said that they have over 100 applications installed on their devices.

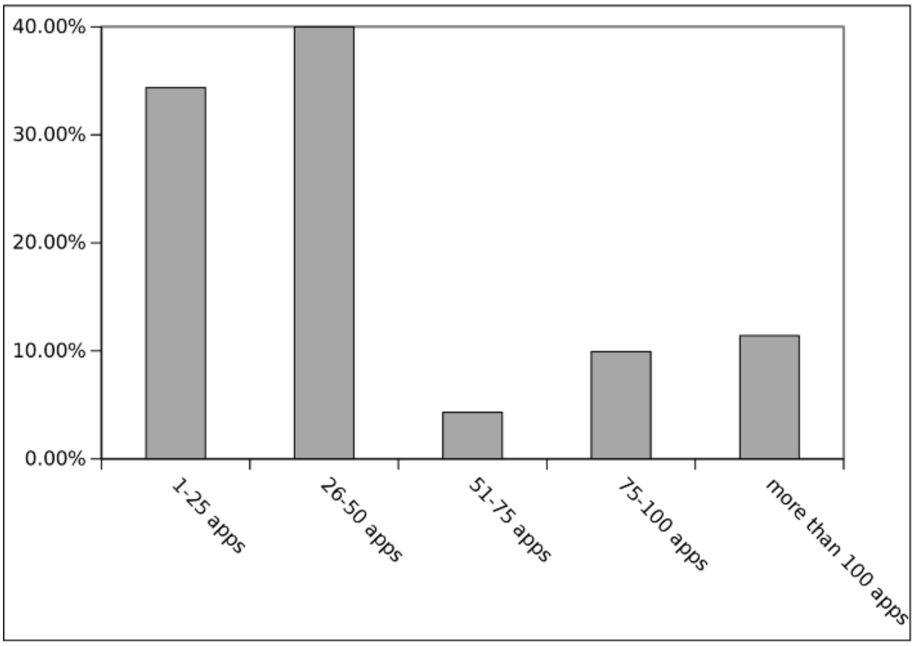

Fig. 2. Number of Applications Installed on Respondents Devices

Table 2. Number of Applications Installed on Respondents Devices

Number of Applications	Number of Respondents	Percentage
1-25 apps	1384	34.37%
26-50 apps	1610	39.98%
51-75 apps	173	4.30%
75-100 apps	400	9.93%
more than 100 apps	460	11.42%

In response to question five; "Which type of data do you consider most private?", the highest percentage of 35.71% was for Photos and Videos. Emails came as second most private data type with 18.52%, which was close to the third type, Passwords Stored on the Device, with 17.18%. These results can be found in Table 3 and Figure 3. Respondents who chose "Other" mostly cited application-specific data as their most private like WhatsApp conversations, Viber conversations, Evernote notes, etc.

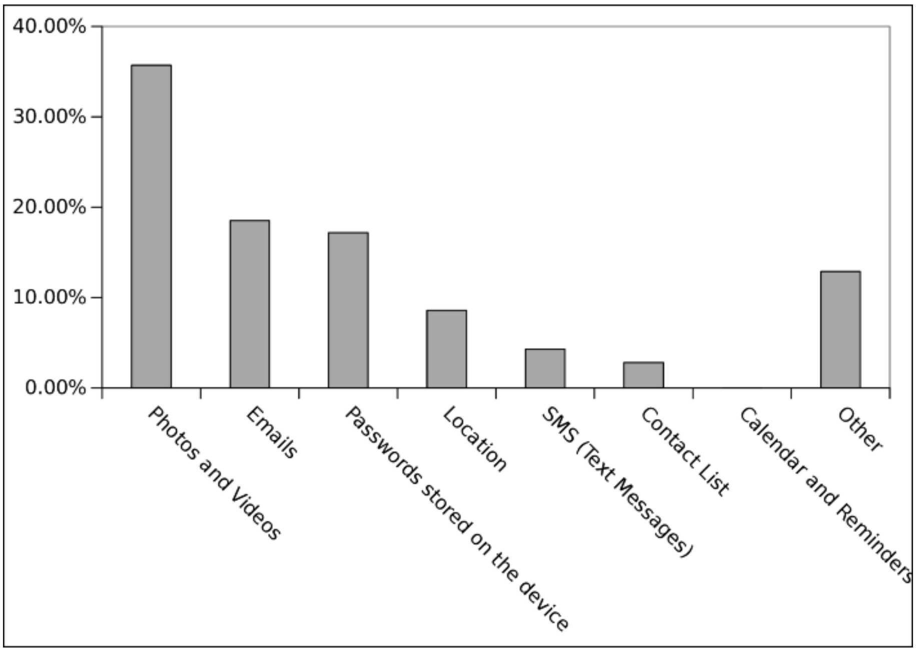

Fig. 3. Most Private Data Types

Table 3. Most Private Data Types

Data Type	Number of Respondents	Percentage
Photos and Videos	1438	35.71%
Emails	746	18.52%
Passwords stored on the device	692	17.18%
Location	346	8.59%
Text Messages	173	4.30%
Contact List	113	2.81%
Calendar and Reminders	0	0.00%
Other	519	12.89%

In response to the sixth question, 68.61% of respondents said that they do not know exactly how many applications have access to their most private data type, while 31.39% said that they know exactly how many applications have access to their most private data type.

Responses to question 7 can be found in Figure 4 and Table 4. The responses show that only 35.71% of respondents read the permissions required by all the applications they install, while 11.42% of respondents never read the permissions.

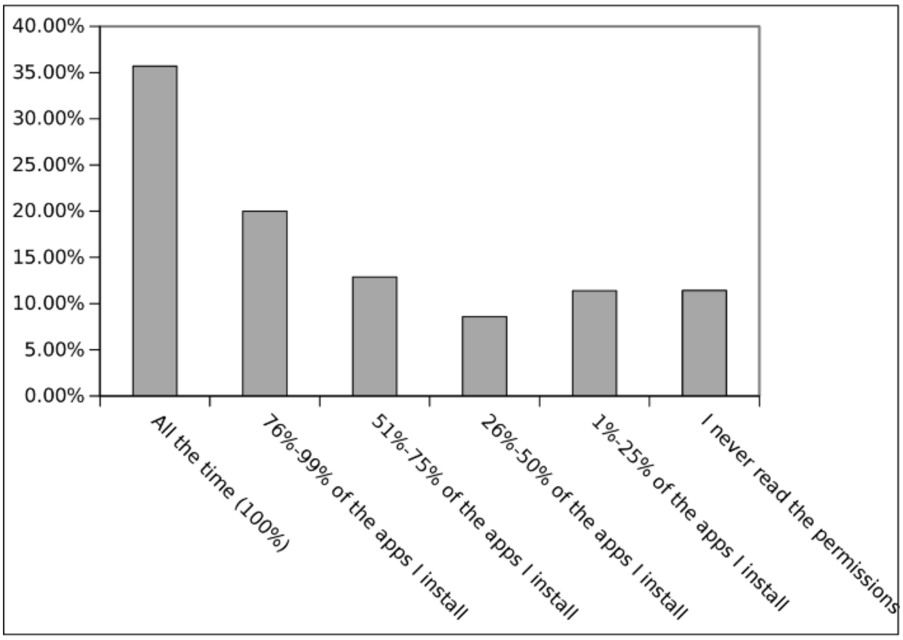

Fig. 4. How often Do You Read the Permissions Of Applications You Install

Table 4. How often Do You Read the Permissions Of Applications You Install

Applications	Number of Respondents	Percentage
All the time (100%)	1438	35.71%
76%-99% of apps	805	19.99%
51%-75% of apps	519	12.89%
26%-50% of apps	346	8.59%
1%-25% of apps	459	11.40%
I never read the permissions	460	11.42%

Responses to question 8 showed that 77.2% of respondents have at least once refused to install an application because of the permissions it's asking for, while 22.8% respondents have never refused to install an application due to its permission requests.

In response to question 9, only 48.6% of the respondents said that they did not use permission controls applications like AppOps, and XPrivacy. The remaining 51.4% respondents said that they have never used such permissions control applications.

Responses to question 10 can be found in Table 5 and Figure 5. These responses show that a high number of respondents have installed many applications that require excessive permissions that do not explain the reason behind asking for these permission.

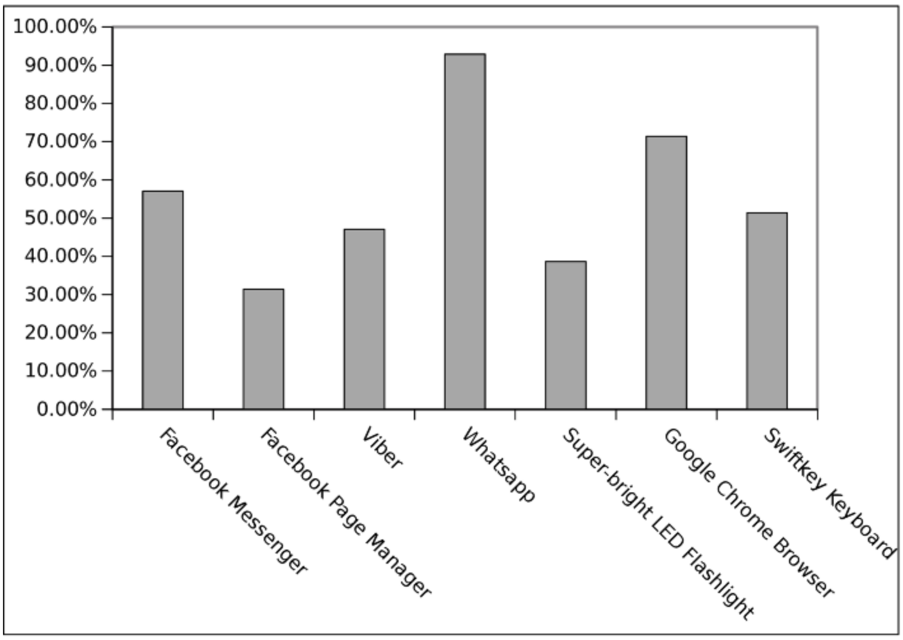

Fig. 5. Which Application(s) Are Installed On Your Device

Table 5. Which Application(s) Are Installed On Your Device

Applications	Number of Respondents	Percentage
Facebook Messenger	2297	57.04%
Facebook Page Manager	1265	31.41%
Viber	1896	47.08%
Whatsapp	3740	92.87%
Super-bright LED Flashlight	1557	38.66%
Google Chrome Browser	2875	71.39%
Swiftkey Keyboard	2070	51.40%

In response to question 11, only 37.17% respondents said that they have previously used, or currently using, anti-malware or anti-virus software on their Android mobile phones, while 62.83% respondents have never installed such software.

None of the survey respondents said that they have been infected 11+ times by a virus or malware in response to question 12. While 69.93% of respondents said that their devices have never been infected with malware or virus, 21.48% said that their devices got infected 1-5 times, and 8.59% said that their devices were infected 6-10 times before.

In response to the last question, number 13, 51.43% respondents said that they have installed applications from external sources other than Google Play Store. The remaining 48.57% said that they have never installed applications from outside of the Google Play Store.

5 Results Discussion

Responses to the first question show an expected distribution over the different versions of Android. However, we expected to see less Android 6 devices as it is the latest model and has not been widely available to older devices.

Responses to the second question have shown that around 54% of respondents' devices were rooted. Root access, can be a very dangerous if the user does not pay close attention to the applications he/she assign root permissions. What makes it more dangerous, is that responses of question 3 show that 48.95% of respondents with rooted devices do not know exactly how many applications on their devices are granted root access. Granting arbitrary root access to applications without understanding the full scope of that access can cause disastrous results in terms of privacy and security in general. In the Previous Work section, we have discussed how some malware can become virtually impossible to remove (even by factory reset) when it get root access [4]. In general, device that are not rooted, have an additional protection layer as compared to rooted devices.

As shown in the previous section, responses to question 4 have shown that 74.35% of respondents have less than 50 applications installed on their devices. Although this information does not directly affect the target of this survey, it shows that most users tend to use a limited set of applications that they are used to and do not explore a lot of applications that they find unnecessary.

Responses to question 5 about the most private type of data, Photos and Videos ranked first with 35.71% while Emails ranked second with 18.52%. Passwords stored on the device ranked only third with 17.18%. These results have shown that the highest percentage of respondents care more about the privacy of their photos and videos than about the secrecy of the passwords stored on their device. The danger of losing stored password can be online banking passwords, email passwords, social media accounts passwords,..etc. did not matter to 82.82% of the survey respondents. Although most of these passwords are encrypted, combining this danger with arbitrary root permissions to any application asking for root access can lead to severe privacy violations. Some users cited application-specific data in the "Other" choice like Facebook Messenger chat, WhatsApp conversations, and Viber conversations. in general, the responses to this question have shown that most users lack awareness of proper priorities of privacy of their data.

Question 6 was connected to question 5 in asking respondents whether they know exactly how many applications have access to their most private data type. A shocking result of 68.61% respondents saying that they do not know exactly how many applications installed on their device have access to their most private data. This indicates that many users either do not read the permissions required by an application or they just ignore it.

Responses to question 7 have shown big weakness in awareness of users about their privacy. Responses have shown that only 35.71% of users read the permissions required by the applications for every application they install. Results also have shown that 11.42% of respondents have never read the permissions required by the application, which can be a very dangerous behavior. When a user does not read the required permission, he/she is voluntarily giving access to what might be malicious software to his/her device. Users must keep in mind that there is no thorough monitoring and testing process for all the applications published through the Google Play Store.

In high relevance to question 7, question 8 asks the respondents if they have ever refused to install an application because of the permissions it is asking for. Responses have shown that 22.8% have never refused to install an application because of its permissions. Although this number is much lower than the 77.2% that have at least once refused to install an application because of its permissions, it is still a high number. Users who install applications without weighing the advantages and disadvantages of each application are also vulnerable to more malware infections.

Responses to question 9 have shown that 48.6% of the users did not use permission controls applications like AppOps or XPrivacy. Although these applications give finer control over permissions on individual application level, not using them does not necessarily mean that those users have no control over the privacy of their data. For example, in Android 6, permissions can be controlled on individual application level and the same results obtained by using AppOps or XPrivacy can be obtained with a built-in feature of the operating system.

The use of permission control application has the advantage of installing the applications that you need without caring much about the required application as later you will be able to control which permission is given to the application and which permission is denied. The disadvantage of using such permission control applications is that some experience is usually required to guarantee that the permission the user is going to deny does not hinder the purpose and performance of the controlled application.

The applications that were selected for question 10 were picked based on the controversy they created due to the excessive permission they ask for. Some of these permission cannot be explained in connection to the purpose of the application.

Responses to question 10 have shown that an application called "Super-bright LED Flashlight" was installed by 38.66% of the survey respondents. This application was discussed in a report in 2015 that have shown that this is the worse "Flashlight" application in terms of the unexplainable permission requirements [19]. The report showed that this application requires 20 different permissions including permissions that are not related to the task the application was design to do. Permissions like "view network connections", "full network access", "read phone status and identity", "approximate locations", "precise location", "modify or delete contents from your USB storage", in addition to several others, can be used for adware and other similar malicious activities. Although the application was later updated with less permission requirements, the fact that it has over 100 million downloads with an average rating of 4.6

out of 5 by over 6 million reviews show a great lack of awareness in the users' community [20].

Responses to question 11 stated that 62.83% users have never used anti-virus or anti-malware software on their Android devices. There have been many studies measuring the effectiveness of this type of applications, and undermining their overall protective capabilities. However, when combining the lack of security software with other dangerous actions like installing applications from outside of the Google Play Store, not reading the permissions of applications before installing them, or giving root permissions to any application that asks for it, can cause a lot of harm to the security and privacy of the users' data.

In response to question 12, 30.07% users said that their device have been infected with malware or a virus before. Although this number is close to many reports about malware-infections in PCs [21], the threat of malware can cause more damage in mobile phones due to the higher level or privacy of data stored on smart phones. When combining this number with the number of users who are using, or have used, anti-virus or anti-malware software, the result is that many other devices might be infected without users' knowledge because of the lack of proper means of detection.

Responses to question 13 state that 51.43% of respondents have previously installed applications from outside of the Google Play Store. Many security reports suggest that 70%-80% of malware is distributed through commonly used applications that are re-packaged with malware and distributed through external channels other than the Google Play Store [4]. Although Google Play Store does not provide a thorough mechanism of malware-checking before publishing applications to users, it is still more secure to install application from the store than from other channels.

Looking into responses of individual question might not be adequate to measure the awareness of users. When we look at all the combined results, we can formulate a user profile that has some serious indicators about lack of awareness. This lack of awareness can lead to serious security and privacy violations. Malicious attackers are building most of their success on this lack of awareness. Users can make the job of the attackers much harder by following basic rules to protect their privacy. Simple steps like installing applications only from Google Play Store, and not rooting their Android device, among other steps, can reduce the probability of malicious infections.

Google also should help in protecting the users for malicious attackers. Not having a proper screening process for application being published on the Google Play Store is a major factor of malicious infections. By not screening, Google is partially participating in the spread of malware amongst Android users. Google is currently implementing a random selection mechanism for testing for malicious content. However, with the rapidly increasing number of applications and replica applications, this loose screening mechanism cannot be trusted to screen all applications. Perhaps, Google should implement a strict screening and testing process similar to the one implemented by Microsoft for Windows Phone applications.

6 Conclusions

In this paper, we publish results of a survey that was done to measure Android users' awareness of privacy and security issues. The results have shown many weaknesses in the awareness of Android users that make them susceptible to various malicious attacks. Based on the results of the survey, we have concluded the following security recommendations:

- Do not root your device unless it is absolutely necessary. Rooted devices are more susceptible to malicious software because of the SuperUser permission it requires.
- If you root your device, do not give root access to all applications requesting it unless you fully understand what this application is trying to do and you are absolutely sure that there is no other way to do it. In addition, make root access time-bound. Some newer root access control application give you the option to grant root access to an application for a limited time like 1 minutes or 5 minutes.
- Do not install applications that you do not use.
- Do not store passwords on your device.
- If you think your data should be private, protect it be not installing applications that ask for unnecessary access to your data.
- Read all the permissions required by each application you want to install. If you cannot understand why this permission is required, do not install the application.
- Google should add a section to their policy that forces application developers to explain why each permission is required in simple non-technical language.
- If you are using an Android version older than 6, install and use permission control applications like XPrivacy and AppOps. These applications give you finer control over permissions on individual application level.
- Although Anti-Virus and Anti-Mawlare applications might not completely protect your device, they do provide a needed layer of security from common malware threats.
- Although not all applications in the Google Play Store are safe, they are definitely safer than installing applications from outside of the store. By installing applications from other channels, you are exponentially increasing the probability of malicious infections.

7 References

[1] Statistica, "Number of smartphone users worldwide from 2014 to 2019 (in millions)," 7 June 2016. [Online]. Available: http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

[2] Gartner, "Gartner Says Worldwide Smartphone Sales Grew 9.7 Percent in Fourth Quarter of 2015," 7 June 2016. [Online]. Available: http://www.gartner.com/newsroom/id/3215217.

[3] PhoneArena, "Android's Google Play beats App Store with over 1 million apps, now officially largest," 7 June 2016. [Online]. Available: http://www.phonearena.com/news/

Androids-Google-Play-beats-App-Store-with-over-1-million-apps-now-officially-largest_id45680.

[4] D. Goodin, "New type of auto-rooting Android adware is nearly impossible to remove," 9 June 2016. [Online]. Available: http://arstechnica.com/security/2015/11/new-type-of-auto-rooting-android-adware-is-nearly-impossible-to-remove/.

[5] Dr.Web, "Android.Spy.277.origin," 7 June 2016. [Online]. Available: http://vms.drweb.com/virus/?is=1&i=8020079.

[6] G. Dan, "Malicious apps in Google Play made unauthorized downloads, sought root," 9 June 2016. [Online]. Available: http://arstechnica.com/security/2016/01/malicious-apps-in-google-play-made-unauthorized-downloads-sought-root/.

[7] T. Isohara, K. Takemori and A. Kubota, "Kernel-based Behavior Analysis for Android Malware Detection," in Computational Intelligence and Security (CIS), 2011 Seventh International Conference on, 2011. https://doi.org/10.1109/cis.2011.226

[8] M. Grace, Y. Zhou, Q. Zhang, S. Zou and X. Jiang, "RiskRanker: scalable and accurate zero-day android malware detection," in Proceedings of the 10th international conference on Mobile systems, applications, and services, 2012. https://doi.org/10.1145/2307636.2307663

[9] J. Sahs and L. Khan, "A Machine Learning Approach to Android Malware Detection," in Intelligence and Security Informatics Conference (EISIC), 2012 European, 2012. https://doi.org/10.1109/eisic.2012.34

[10] A. Desnos, "Androguard," January 2011. [Online].

[11] B. P. Sarma, N. Li, C. Gates, R. Potharaju, C. Nita-Rotaru and I. Molloy, "Android Permissions: A Perspective Combining Risks and Benefits," in Proceedings of the 17th ACM Symposium on Access Control Models and Technologies, 2012.

[12] D. J. Wu, C. H. Mao, T. E. Wei, H. M. Lee and K. P. Wu, "DroidMat: Android Malware Detection through Manifest and API Calls Tracing," in Information Security (Asia JCIS), 2012 Seventh Asia Joint Conference on, 2012. https://doi.org/10.1109/asiajcis.2012.18

[13] Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution," in 2012 IEEE Symposium on Security and Privacy, 2012. https://doi.org/10.1109/SP.2012.16

[14] Z. Aung and W. Zaw, "Permission-based android malware detection," International Journal of Scientific and Technology Research, vol. 2, pp. 228-234, 2013.

[15] B. Amos, H. Turner and J. White, "Applying machine learning classifiers to dynamic Android malware detection at scale," in 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), 2013.

[16] S. Sheen and A. Ramalingam, "Malware Detection in Android Files Based on Multiple Levels of Learning and Diverse Data Sources," in Proceedings of the Third International Symposium on Women in Computing and Informatics, 2015. https://doi.org/10.1145/2791405.2791417

[17] Z. Cai and R. H. C. Yap, "Inferring the Detection Logic and Evaluating the Effectiveness of Android Anti-Virus Apps," in Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy, 2016. https://doi.org/10.1145/2857705.2857719

[18] LimeSurvey, "LimeSurvey," 7 June 2016. [Online]. Available: https://www.limesurvey.org/.

[19] SnoopWall, "FLASHLIGHT APPS THREAT ASSESSMENT REPORT," 7 June 2016. [Online]. Available: http://www.snoopwall.com/wp-content/uploads/2015/02/Flashlight-Spyware-Report-2014.pdf.

[20] Surpax, "Super-Bright LED Flashlight," 20 June 2016. [Online]. Available: https://play.google.com/store/apps/details?id=com.surpax.ledflashlight.panel.

[21] J. P. Mello, "Report: Malware Poisons One-Third of World's Computers," 20 June 2016. [Online]. Available: http://www.technewsworld.com/story/80707.html.

8 Author

Mohammed M. Alani is an Associate Professor of Computer Engineering. He works as the Provost in Al-Khawarizmi International College in Abu Dhabi, United Arab Emirates. He has served as a member of many international committees in different journals and conferences. (email: m@alani.me).

Article submitted 30 December 2016. Published as resubmitted by the author 14 February 2017.