International Journal of Engineering & Technology, 7 (1.1) (2018) 297-300

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A detailed study on risk assessment of mobile app permissions

D. Naga Malleswari [1] *, A.Dhavalya [2], V.Divya Sai [2], K.Srikanth [2]

[1] Professor Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation,Vaddeswaram, Guntur, Andhra Pradesh, India-522502
[2] Student Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India-522502
**Corresponding author E-mail: dhavalya.cse@gmail.com*

Abstract

Mobile phone have user's personal and private information. When mobile applications have the permission to access to this information they may leak it to third parties without user's consent for their own benefits. As users are not aware of how their personal information would be used once applications are installed and permissions are granted, this raises a potential privacy concern. Therefore, there is a need for a risk assessment model that can intimate the users about the threats the mobile application poses to the user's private information. We propose an approach that helps in increasing user's awareness of the privacy risk involved with granting permissions to Android applications. The proposed model focuses on the requested permissions of the application and determines the risk based on the permission set asked and gives a risk score.

Keywords: *Risk Assessment; Android; Applications; Privacy Leakage; App Permissions.*

1. Introduction

Mobile phones have become a part and parcel in our daily lives. With the rapid increase in usage of android mobile phones, there is a stark increase in the variety of android applications available to people. Android phones are equipped with various features like video/camera, location, messaging services, mail accounts and many more. Therefore there always resides the concern of losing the personal information we feed in our phones. The increase mobile phone functionalities is resulting in a parallel increase in the privacy risk to the user. From security point of view we see that this private information of users is being manipulated by the third parties through android application and the permissions they ask for [7]. Mobile applications take permissions to have access to these device resources and hence these are a constant threat to user. In the present scenario, users are forced to accept various permission requests for being able to use the app. Smart phones these days are preferred over desktops. A study notes that most people use these phones for easy cash transactions, games, messaging purpose or the social networking and web browsing [11]. They have respective applications for all different usages.

The mobile applications vendors are taking the advantage of this situation, and are imposing a threat to our privacy for their own profits [4]. They may leak this data to a third party without the user's approval. Constant monitoring of the user and his activities can also be done by these applications. They ask for permissions that are not necessarily required to steal the user data. The other side of the coin in these leakages is the user's unawareness. The reasons of this unawareness include blind trust in the application [2] [3]. But considering the slow adaption of the users to the ever changing technologies, there is a need for the tool or framework that assess this risk. We in our paper, present a deeper insight to these data leakages in the smart phones through these mobile application permissions. We also propose a model which will calculate the risk score of the application thus providing an awareness of data leakage risk to the user.

2. Problem statement

Mobile applications take permissions to have access to these device resources. The mobile applications vendors are taking the advantage of this situation, and are imposing a threat to our privacy for their own profits. They may leak this data to a third party without the user's approval. Constant monitoring of the user and his activities can also be done by these applications. They ask for permissions that are not necessarily required to steal the user data. We see that this sensitive information of users is being manipulated by the companies through android application and the permissions they ask for [15]. Considering the slow adaption of the users to the ever changing technologies, there is a need for the tool or framework that assess this risk.

3. Understanding the risk scale of different permissions

3.1. Connect and disconnect from Wi-Fi

This permission is used to receive messages - video or text or files under various network conditions like mobile data or Wi-Fi. It is also usually asked for automatic updating of apps in presence of Wi-Fi, and update is asked for user's consent in the case of mobile data usage. This permission constitutes the risk of a hacker taking advantage and stealing Wi-Fi passwords. It is requested by almost all the applications. There is no much risk to user's privacy in letting apps have this permissions. Therefore a negligible severity is assigned to this permission.

Examples of Apps which ask for this permission are Amazon, UC Browser, Daily Hunt, Subway Surfers etc.

3.2. Contacts

This permission is used to match phone numbers with their respective names and to display the contact information when you are composing messages on the application. There will be several passwords and account numbers associated with our contacts and access to contacts leads to a privacy risk of our personal information. In some instances mails are also linked to the contacts so there are high chances of data getting leaked and getting spam messages. The apps like Paytm, Airtel use contacts mainly because they can transfer money by simply using mobile number if the third party tries to access the contacts in middle then it would be a threat to the person using that app unless cases where user stores private information in his contacts . The severity is negligible unless cases where user stores private information in his contacts.

3.3. Identity

This permission gives access to find accounts, to check for contacts. It can manipulate the contacts by creating new ones or by modifying existing ones .There will be less risks associated with the identity it helps us to identify the contacts when we are getting incoming call that time our contact list will be referred in order to determine the name of person. Social messaging apps ask for this permission.

3.4. Location

It tells where the person is located at. It also assists us in finding certain places which we are unaware of. This permission grants apps access to your exact location and can be abused by developers to make money through the location based apps. Malicious apps use it to load location-based attack or malware. A person can be easily traced with the help of location permission. We propose a limited risk scale to this. Apps like Taxi apps use this kind of permission.

3.5. SMS

This permission is used to receive Messages or Multimedia Messages under different network conditions. Abusers use this permission to send messages thus resulting you unwanted additional charges. Many Cybercriminals can also use it to communicate to command centres. As this permission also allows you total access on receiving messages, several personal information will be leaked if affected. For example, bank OTPs you recieve can be read and accessed by the cybercriminals leading you to huge irreversible damages.
Apps like Facebook, Hike, Whatsapp, OLX ask for this permissions.

3.6. Storage

When you receive incoming image, video, or audio messages these are stored locally on your device. This permission is necessary in order to enable import export functionality. Cybercriminals use this to store copies of stolen information or to save files onto your SD card. Malicious apps can also delete these images and other personal files on your SD card. We propose level 2 scale of danger to this permission. Apps like camera apps, audio and video apps, document apps.

3.7. Retrieve running apps

This lets the applications to identify currently or recently running tasks and the processes running for each one. Hackers use this permission to steal information from other running apps. They can also check for and kill security apps .We propose a limited risk scale to this permission. Applications which mainly ask this kind of permission are task killer apps, battery monitoring apps, security apps.

3.8. Control vibrator

This permission gives access to the device vibrator function. Usually various notifications are identified with the help of control vibrator.
Malware applications use it to stop vibrations and try to control them these can help us to alert you of any incoming messages. It is not dangerous to identity and we give it a level 1 score. Applications that need this permission are communication apps, gaming apps.

3.9. Prevent from sleeping

This permission prevents the processor from sleeping and from lowering the light of the screen. This will be active when any applications are running in background. As a result there will be an extra drainage of battery. Malware applications prevent the phones from going to sleep mode, so that they can continuously run malware activities in the background. This can harm our mobile phone and is a potential risk as the damages done may or may not be retraceable. Therefore we give a level 3 score to this permission.
Apps that need this permission are audio and video apps, gaming apps, browser apps

3.10. Photos/media/files

This permission in order to access the gallery, audio and file databases. It is generally asked by apps which allow users to transfer media. Privacy risk arises when database is corrupted otherwise it is not much a risk. So we give a limited score to this permission.
Apps like Photoediting, Instagram, Whatsapp etc. generally ask such permissions.

3.11. Calendar

This permission don't hold much risk effect as many social media news applications mainly use this to helps remind about particular events.
These kind of permission doesn't affect user's privacy and can be given a negligible risk score. Apps ask this permission to mark events.

3.12. Run at startup

This is enabled when the phone first starts up and before the user has entered their password. Without this, there may be a delay in receiving messages. The applications start in the root itself. Malware applications use this to automatically run at every boot. Any personal accounts in the database can be easily effected by these malicious applications.
Applications which ask this mainly are 360security, UC Browser etc. mainly ask this type of permission.

4. Model design

The risk score calculator model consists of 5 steps:

4.1. The total number of permission scale

The total number of permissions asked by the application can be the initial and foremost step in assessing the risk. The risk is directly proportional to the number of permissions asked. The scale is determined using EBIOS method. EBIOS is privacy risk assessment method by a French data protection authority. Its aim is

to ensure that the privacy of data is implied to collection, storage and usage. We focus on the second phase which is focussed on the feared events in particular context. We divide on level basic where the lower number in level tells it's less risk and a higher one determines its severity. There are four levels the scale goes as:

<3	Level1
<5	Level2
<7	Level3
>10	Level4

4.2. User choice

We take in the user's decision on determining which resources and what data he wants to keep private, Thus enabling a more personalized risk score. We in took this case into consideration as a study shows that people have different privacy opinion on the same data. For suppose, person 'A' maybe okay with disclosing his birthday as he expects gifts from family and friends. But, some person 'B' is not okay with disclosing his birthday detail as he has set some password related to his birth date. There may be some people who save their bank account details in contact book. Permission risk severity may differ from person to person. So, to even consider risk in such cases we come up with this user personalized risk score calculation method.

4.3. Potential risk calculation of the permissions individually

Based on the detailed survey study above, we give a risk level to each individual permission. The factors considered are identity disclosure of the user and the level of damage caused by potential impacts. [5] We calculate the risk by adding the assigned score of level determined on the basis of these two attributes.
The individual permission risk is calculated by:

score (p.i) = (levelscore1.i + levelscore2.i) / 2;

Where,
i = permission number;

The score of the individual permissions is given and they are integrated to get the score of this phase:
Phase 2 score = (∑p. i) / n; where i ranges from 1 to n
n= number of permissions

4.4. The actual requirement of that permission in that particular genre of applications

We have to determine the importance of the permission in that particular genre of apps so as to know its importance and thus determine the risk. This is a Multi Criteria Decision making kind of problem. We consider Analytical Hierarchy Process (AHP) which was introduced by Saaty [17] [18] to solve this. It is mainly chosen because of its mathematical properties and also the ease of obtaining the input data.
For each permission (Pi), we calculate the relative average number of occurrences of permissions in that genre of apps. The test data may range in some thousand apps calculation, thus giving a more accurate relation to the importance of that permission in that app.

4.5. The risk of interactions between permissions

Permissions tend to prove more risky when they interact with other high risk score permissions. We use the phase 2 level scores to determine the higher risk associated with the permission set of app. If the app consists more than one level 4 permission, it risk score increases. We should always consider the cases of higher data leakage scenarios. With more number of higher level permissions in permission set, the data leakage and privacy risk increases more. Having more permissions of level 4 impacts the risk score of the app. Since interaction means combination of two or more permissions, we propose to compute interaction severity as a sum of level indicators.
The risk score is obtained from the integration of 5 phases scores.

5. Implementation results

We analyzed various apps and calculated their respective risk scores. We present in this section our findings on apps in terms of score.

S. No	Application Name	Score
1.	Paytm	6.2
2.	Bill Payment And Recharge	3.7
3.	Dream11 Pro Expert	2.8
4.	Cricbuzz	4.5
5.	Tv9	4.8
6.	Dailyhunt	4.5
7.	Eenadu News	3.3
8.	Messenger	4.5
9.	Instagram	4.3
10.	Linkedin	4.2

6. Conclusion

This paper presents a research on privacy issues related to Android applications permissions granting which is considered as a cause of privacy leakage. A privacy risk assessment model was proposed to assess the risk to users' privacy during the granting of permissions required by mobile applications.
The parameters considered include the individual permission risk assessment and risk of their interactions and the relative importance of the permission. We also consider the user's opinion in permission risk determination. The determination of the relative importance have been formulated as MCDM problem and solved using the AHP method. We used different scales to determine the scores. Thus our model succeeds in detecting the permissions required by an application and to estimate the risk of the application very before its installation. It creates awareness among users and helps them in deciding regarding permission granting while taking into account the risk score of the application. This would also contribute to encourage applications developers to seek access to only required resources and permissions.

7. Future work

The major setback of our model is that it only considers the apps permission set as risk attributes. Although, the permission set is an efficient estimator for risk assessment it is not totally sufficient. There can be cases where the virus or malware exists and cannot be recognized only by considering the permission set [6]. For example, root exploits which clearly are a risk doesn't need the permissions as they only require the ability to execute code and therefore such cases of risks are failed to be estimated in our model [8].
We plan to additionally consider other risk signals than permission sets like code risk analysis of the applications. Furthermore, we plan to enhance the existing permission based score plan.

References

[1] Wei Wang, Xing Wang, Dawei Feng, Jiqiang Liu, Zhen Han, and Xiangliang Zhang , "Exploring Permission-induced Risk in Android Applications for Malicious Application Detection " in IEEE transactions on information forensics and security in 2015
[2] Mylonas, A., et al., A qualitative metrics vector for the awareness of smartphone security users, in Proceedings of Trust, privacy, and security in digital business, 2013, pp.173-184.
[3] Mylonas, A., et al., Delegate the smartphone user? Security awareness in smartphone platforms, Computers & Security, 2013, pp.47-66. https://doi.org/10.1016/j.cose.2012.11.004.

[4] Google: Privacy policies for android apps developed by third parties 2013, Retrieved 2016, from https:// support.google.com/googleplay/answer/2666094?hl=en
[5] Commission Nationale de l'Informatique et des Libertés (CNIL), Methodology for Privacy Risk Management, 2012.
[6] Gibler, C. et al., Androidleaks: Automatically detecting potential privacy leaks in android applications on a large scale, in Proceedings of the 5th International Conference on Trust andTrustworthy Computing, Vienna, Austria, 2012. https://doi.org/10.1007/978-3-642-30921-2_17.
[7] T.-E. Wei, A. B. Jeng, H.-M. Lee, C.-H. Chen, and C.-W. Tien, "Android Privacy," in Proc. Int. Conf. Mach. Learn. Cybern., Xian, China, Jul. 15–17, 2012, pp. 1830–1837.
[8] T. Isohara, K. Takemori, and A. Kubota, "Kernel-based behavior analysis for android malware detection," in Proc. 7th Int. Conf. Comput. Intell.Security, 2011, pp. 1011–1015. https://doi.org/10.1109/CIS.2011.226.
[9] M. Tschersicha et al., "Towards privacy-enhanced mobile communities— Architecture, concepts and user trials," J. Syst. Softw., vol. 84, no. 11, Nov. 2011. https://doi.org/10.1016/j.jss.2011.06.048.
[10] W. B. Tesfay, T. Booth, and K. Andersson, "Reputation based security model for android applications," in Proc. IEEE 11th Int. Conf. Trust, Security Privacy Comput. Commun, 2012, pp. 896–901. https://doi.org/10.1109/TrustCom.2012.236.
[11] N. A. Mutawa, I. Baggili, and A. Marrington, "Forensic analysis of social networking applications on mobile devices," Digit. Investigation, vol. 9, pp. 24–33, Aug. 2012. https://doi.org/10.1016/j.diin.2012.05.007.
[12] A. Shabtai and Y. Elovici, "Applying behavioral detection on androidbased devices," in Proc. Mobilware, vol. 48, Lecture Notes of the Institute for Computer Sciences, 2010, pp. 235–249.
[13] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in Proc. 1st ACMWorkshop SPSM, Chicago, IL, USA, 2011, pp. 3–14.
[14] Y. Nadji, J. Giffin, and P. Trayno, "Automated remote repair for mobile malware," in Proc. 27th ACSAC, 2011, pp. 413–422. https://doi.org/10.1145/2076732.2076791.
[15] M. Landman, "Managing smart phone security risks," in Proc. InfoSecCD, 2010, pp. 145–155.
[16] G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, "Paranoid android: Versatile protection for smartphones," in Proc. 26th ACSAC, 2015, pp. 347–356.
[17] Triantaphyllou, E. and Mann, S.H., Using the Analytic Hierarchy Process for decision making in engineering applications: some challenges, International Journal of Industrial Engineering: Applications and Practice, 1995, 2(1), pp.35-44.
[18] Saaty, T.L., Decision making with the analytic hierarchy process, International journal of services sciences, 2008, 1(1), pp.83-98. https://doi.org/10.1504/IJSSCI.2008.017590.