A Proactive Approach toward Privacy Risk Assessment for Android Apps Permissions

Asma Hamed
CRISTAL Lab.
National School of Computer Science
University of Manouba
Manouba, Tunisia

Esprit School of Engineering
Tunis, Tunisia

hamed.asma@gmail.com

Hella Kaffel-Ben Ayed
CRISTAL Lab.
National School of Computer Science
University of Manouba
Manouba, Tunisia

Faculty of Science of Tunis
University of Tunis El Manar
Tunis, Tunisia

hella.kaffel@planet.tn

Dorra Machfar
Faculty of Science of Tunis
University of Tunis El Manar
Tunis, Tunisia

dorra.machfar@yahoo.com

Abstract— **Mobile devices store users' personal data. When mobile applications have access to this data they may leak it to third parties without users' consent. Google's Android platforms include a permission model that restricts applications' access to users' personal data. However, users are not aware of how their personal data would be used once applications are installed and permissions granted. This raises a potential privacy concern. In this paper we propose a proactive approach towards users' awareness of the privacy risk involved with granting permissions to Android applications. We present a dynamic privacy risk assessment model that assesses the risk to users' privacy associated to an application which requires a set of permissions. The parameters of this model are the severity and the relative importance of permissions and their interactions. Severity is evaluated according to a standard severity assessment method. The relative importance is estimated according to an analytic method. An experimental study to validate our proactive approach has been conducted. The originality of this works lies in that the privacy risk for a given device owned by an individual varies dynamically based on its different uses applications and related permissions.**

Keywords—risk assessment; Android applications; Android permissions; privacy

I. INTRODUCTION

Mobile devices have become more efficient and widespread. They are often used as personal assistants, banking terminals, memory-extenders, trainers, etc. They are equipped with many capabilities such as GPS, SMS & MMS sending, camera, etc. Mobile devices carry a growing amount of personal data such as users' location, unique identifiers, banking data and pictures. Mobile applications (apps) have access to the device's resources. They acquire, consume and distribute users' data. In Google's Android platforms, access to devices capabilities is protected via a permission model. Each application, before being installed, asks for a set of permissions in order to access restricted resources [1]. In the literature, studies have shown that Android users ignore permissions, or do not understand them at all [24,25]. Users should be able to review an app's privacy policy prior to downloading it and the policy must clarify what types of data are collected and for which purpose. However, in Google Play the inclusion of such a policy is not mandatory for app developers [26]. Thus, this way of working does not inform users how their mobile device's resources and their personal data would be used once permissions are granted. Privacy violations may occur if users' activities and personal data are leaked to third parties without their knowledge or consent. Currently the assessment of privacy risks in Android apps lacks a proactive approach that enhances users' awareness before the installation of an application, i.e. before the leakage occurs. The goal of this work is to address this issue. We propose a proactive approach toward users' awareness of the privacy risk involved with granting permissions to Android applications. Our methodology consists of three steps: 1) the proposal of a dynamic privacy risk assessment associated to an Android application. The model aims to enhance users' awareness of the risk to their privacy. The parameters of our model are the severity and the relative importance of permissions and their interactions. 2) The development of an application, i.e. PrivacyAndroid, that

978-1-5090-4372-9/17/$31.00 ©2017 IEEE

implements the model and computes the privacy risks estimation upon installing applications. 3) The validation of the proposal. We conduct an experimental study on applications and required permissions using both our new proactive approach and an existing reactive approach. Finally, we compare the obtained results to validate our work.

The remainder of this paper is organized as follows: section II presents related works. Section III presents the privacy risk assessment model. Section IV presents our privacy risk assessment application. Section V presents the validation of our work. Finally, Section VI concludes the paper.

II. RELATED WORKS

We categorize related works into three types: tools based, quantification, and risk assessment based approaches.

A. *Tools Based Approaches*

The work in [2] presents TaintDroid, a tool used to monitor the behavior of 30 popular third-party Android applications. The study shows suspicious handling of sensitive data in two-thirds of the applications. Users' locations have been reported to advertising parties in one half of the applications. Authors in [3] perform a similar analysis with another tool, AndroidLeaks. 24,350 Android applications from several Android markets are analyzed. AndroidLeaks found 57,299 potential privacy leaks in 7,414 Android applications. 2,342 applications leak private data including phone information, GPS location, WiFi data, and audio recorded with the microphone. The study carried out in [4] identifies the correlations between the users' actions and the leakage in order to report the causes from a user's point of view. Leak causes have been identified from logs of users' actions in more than 220 Android applications. Leaks have been detected using TaintDroid [2]. The study shows the following: 47% of the sampled apps leak various kinds of privacy data, more than 60% of the 105 leaky apps leak data as a result of users' actions on certain GUI widgets in the apps. About 44% of the leaky apps also leak data just after being started, while 32% leak data periodically after their start. In [6], the authors present Permlyzer which automatically explores the functionality of an application and analyzes the permission uses. Their evaluation using 51 malware/spyware families and over 110.000 Android applications demonstrated that Permlyzer can provide a detailed permission use analysis. The study carried out by authors in [7] proposes an approach to inform users whether the risk of installing an app is in proportion with its expected benefit based on requested permissions. Authors in [9] present VetDroid, a dynamic analysis platform for reconstructing sensitive behaviors in Android apps from a novel permission use perspective. They applied VetDroid to 1.249 top free apps in Google Play and showed that this tool can be used to analyze fine-grained causes of information leaks that TaintDroid could not reveal.

B. *Quantification Based Approaches*

Authors in [5] present an alternative approach to provide the users with the knowledge needed to make informed decisions about the applications they install. They created a knowledge base of mappings between API calls and fine-grained privacy-related behaviors. They identified 221 distinct application behaviors for which they created rules. They used this knowledge base to produce, through static analysis, high-level behavior profiles of application behavior. The authors analyzed almost 80,000 applications up to date and made the resulting behavior profiles available both through an Android application and online. Nearly 1500 users have used this base up to date. Based on 2782 pieces of application-specific feedback, they analyzed users' opinions about how applications affect their privacy and demonstrated that these profiles had a substantial impact on their understanding of those applications. In [8], authors constructed rule sets with a decision tree in order to detect malware applications (malapps). The evaluation is performed using a set of 310.926 benign apps and another set of 4.868 malapps. The study shows that risky permissions can be effective for the detection of malapps at least for the first scan of a large amount of Android apps.

C. *Privacy Risk Assessment Based Approaches*

In [10], the authors present a comparative study of methods that allow an organization to assess their information security risk. The main purpose of the study is to compare and clarify the different activities, inputs and outputs required by each security risk assessment models and also analyze which ones address information security risk effectively. In [11] the authors study the differences and limitations of the most common risk assessment frameworks, the conceptual models that support them, as well as the tools that implement them. A total of 14 methodologies, 25 tools and 7 conceptual models have been analyzed, described and reviewed. The main purpose of the study is to better understand the applicability of each method in order to suggest guidelines for picking the most suitable one. Authors in [13] proposed and developed a new qualitative approach for assessing information security risks. The approach provides an easy-to-apply information security risk analysis spanning the enterprise. Authors propose a mathematical formulation of risk by using a lower level of granularity of its elements: threat, probability, criteria used to determine an asset‘s value, exposure, frequency and existing protection measure. In [27] authors propose a targeted risk assessment method to assess user-specific parameters and Smartphone-specific threats. The proposed method is tailored for Smartphones by dividing the device into various (sub) assets, assessing Smartphone specific threats, and taking into account the characteristics of a Smartphone security model. The data analysis takes place transparently to the user and it leads to a personalized risk assessment, as user input details vary according to user skill. In [28] the same authors refine their previous work by describing a method that assesses privacy risk by combining the likelihood of permissions with user input regarding the impact of disclosure. The assessment is based on the impact valuation from the user which enables per user risk assessment. Although the proposed approach is interesting to assess privacy risk in Android, it assumes the participation of users. So it depends on the subjectivity of their impact perceptions which may indeed affect the quality of results. Authors examine two use cases: 1) a teenager who uses his Smartphone for making phone calls, texting, playing games and listening to music 2) A businessman who uses his Smartphone for reading news and magazines, consulting the weather, socializing with colleagues or clients, reading maps and navigating by GPS. Authors propose a dynamic privacy risk assessment that changes according to users' profile (teenager or businessman). For instance the teenager has a greater vulnerability level for the threats that involve access to calling history than the businessman. For threats involving access to the device's location, the businessman's vulnerability level is greater due to his preference to navigation apps. This approach is interesting but highly biased by users' behavior. Furthermore, authors do not consider individual permissions. Their study includes only permission combinations.

All these studies and surveys show that privacy risk is becoming a reality and that Android applications represent a threat for users' privacy. However, to the best of our knowledge there is no study that proposes a proactive approach to improve Android users' awareness regarding privacy when granting resources access to mobile applications.

III. PRIVACY RISK ASSESSMENT MODEL

In a previous work [32], we proposed a dynamic model to estimate the privacy risk upon application installation. This model increases dynamically with the number of granted permissions. The parameters of our model are the severity and the relative importance of permissions and their interactions. The formal definition of the proposed privacy scoring model is presented in (1):

$$PrivacyScoreapp = \sum(\alpha_i * p_i) + \sum(\beta_j * Int_j) \quad (1)$$

α_i represents the relative severity of a permission p_i and β_j represents the relative severity of an interaction Int_j.

We defined the relative severity as the product of the severity and the relative importance. The severity was estimated according to EBIOS [12]. EBIOS is the method for privacy risk assessment by CNIL, the French data protection authority whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data. It describes a complete analytical approach for improving the management of personal data processing risks [29]. The assigned severities were inspired from related works. Then we defined the relative importance of permissions (respectively interaction) as its weight compared to the other required permissions (respectively interaction). The formalized the calculation of the relative importance as a MCDM (multi-criteria decision-making) problem. We relied on the Analytic Hierarchy Process (AHP) a MCDM method that was introduced by Saaty [20,21,22]. Finally, we conducted a preliminary experimental study on 64 Android applications. The data collected during the research were compiled and analyzed with the Statistical Package for Social Science (SPSS) software from IBM [30]. We found that the most required permissions are storage, geolocation, the device ID, the account and personal information access. We studied the number of permissions required by applications. We observed that Facebook, musicyahoo and Tagged leaded the ranking with very close scores. Twitter came next in the ranking. We used our model to compute permissions' and interactions' scores. We observed that the number of permissions was not the unique factor that impacts the scores. Indeed, plus.google had a bigger number of permissions than Twitter and Tagged but had a lower score. This was explained by the fact that the proposed privacy scoring model is based on a quantitative parameter (number of permissions) and a qualitative parameter (the severity of permissions).

The previous study was important to have general statistics about applications and permissions. However, it lacks an implementation and a validation of our privacy risk assessment model.

IV. PRIVACY RISK ASSESSMENT APPLICATION

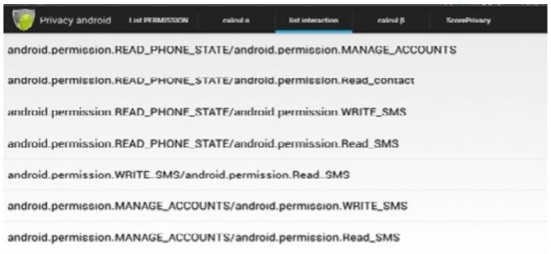
In this work we address the previous mentioned lacks. In a first step, we develop a privacy risk assessment application named PrivacyAndroid that proactively estimate privacy risks upon installing applications on mobile devices. In a second step we use PrivacyAndroid on a set of applications in order to compute their scores. We use a reactive approach on the same set of applications. Finally we validate our model. We compare the results of our proactive approach with those of the reactive approach.

PrivacyAndroid implements the previously defined privacy risk assessment model to compute and display a score that indicates the relative severity of an application before it is installed. The goal of our application is to assess users' awareness by identifying the risks in a proactive manner. Making users' aware about how they are tracked constitutes a first step to privacy provision.

PrivacyAndroid performs the following tasks:

1. Identifies permissions required by applications;
2. Analyses the most risky permissions as well as the interaction between them;
3. Computes their respective scores;
4. Displays the significant results to the user with color codes: green for less risky applications, orange for medium risky applications, red for risky applications and black for extremely risky applications.

Fig. 1 represents a screen shot of PrivacyAndroid.



android.permission.READ_PHONE_STATE/android.permission.MANAGE_ACCOUNTS
android.permission.READ_PHONE_STATE/android.permission.Read_contact
android.permission.READ_PHONE_STATE/android.permission.WRITE_SMS
android.permission.READ_PHONE_STATE/android.permission.Read_SMS
android.permission.WRITE_SMS/android.permission.Read_SMS
android.permission.MANAGE_ACCOUNTS/android.permission.WRITE_SMS
android.permission.MANAGE_ACCOUNTS/android.permission.Read_SMS

Fig. 1. Analysis of permissions and interaction

V. VALIDATION

We present in this section the experimental study conducted to validate our model as well as a discussion of the obtained results.

A. *Experimental Results*

We have conducted an experimental study on a set of mobile apps using our developed application, i.e. PrivacyAndroid. Our validation approach consists in comparing our proactive approach's results with a reactive approach's results. For that purpose we use the PermissionDog application [31] that defines the privacy risk of an application after installation. PermissionDog lists all the applications installed on a mobile device and verifies the permissions required by each application. Each time an application is launched a notification appears and indicates the number of permissions requested by this application and its dangerousness.

We exploit 5 Android mobile devices in the experiment: Evertek, LG, Evertek One touch tab, Huawei Honor6 and Galaxy tab 4. On each of these devices we use PrivacyAndroid to estimate the risk of various applications before installation. We work on 10 mobile applications presented in table I. Similarly, we use PermissionDog to estimate the risk of these same applications after installation. Finally, we compare the results of our proactive approach with those of the reactive approach. This comparison between an already known and used approach with our proposed new approach constitutes the basis of our validation.

TABLE I. MOBILE APPLICATIONS

Applications mobiles
TestApK
AstucesMath
Taalam
Athkar
Download
Winamp
Imo
Quissas
VideoTube
Cordova

Fig. 2 shows the results for the Huawei Honor6 device. The highest scores are those of the AstucesMath application with a PrivacyAndroid score of 5 and a PermissionDog score of 4.7. The imo application gets the lowest score with 0.6 as PrivacyAndroid score and 0.8 as the PermissionDog score.

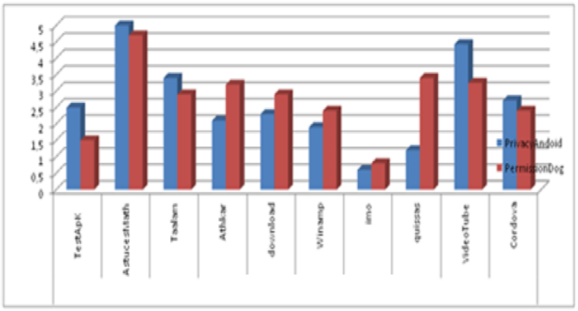


Fig. 2. Huawei Honor6 mobile device

Fig. 3 shows the scores for the Evertek device. The highest scores are those of the AstucesMath app with a PrivacyAndroid score of 3.7 and a PermissionDog score of 4.1. The Winamp and VideoTube applications get the lowest scores with respectively 0.5 and 0.6 as PrivacyAndroid score, 1.1 and 0.98 as the PermissionDog score.

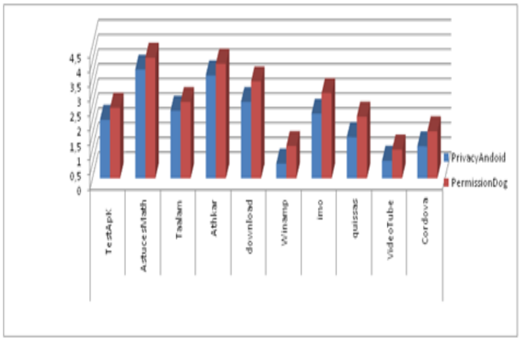


Fig. 3. Evertek mobile device

Fig. 4 shows scores for the LG mobile device. The highest scores are those of the Athkar application with a PrivacyAndroid score of 4.75 and a PermissionDog score of 4.9. The VideoTube app gets the lowest scores with 0.4 as PrivacyAndroid score and 0.6 as the PermissionDog score.

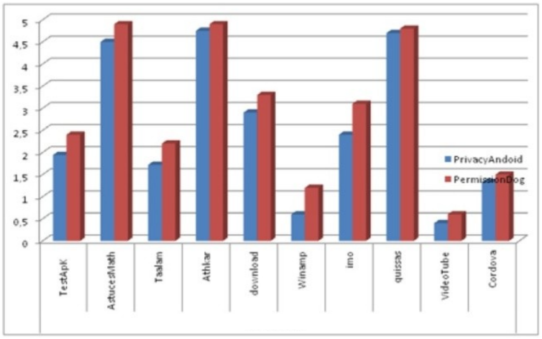


Fig. 4. LG mobile device

Fig. 5 shows scores for the Evertek OneTouch Tablet. The highest scores are those of the AstucesMath app with a PrivacyAndroid score of 4.5 and a PermissionDog score of 4.9. The imo application gets the lowest scores with 0.7 as PrivacyAndroid score and 1.2 as the PermissionDog score.

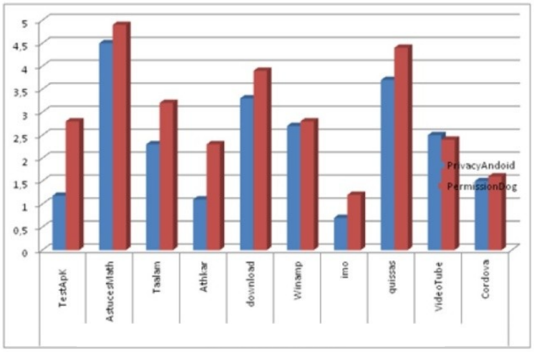


Fig. 5. Evertek OneTouch Tablet

Fig. 6 shows scores for Galaxy Tab 4 tablet. The highest scores are those of the imo application with a PrivacyAndroid score of 3.5 and a PermissionDog score of 4.1. The Taalam application gets the lowest scores with 1.2 as PrivacyAndroid score and 0.8 as the PermissionDog score.

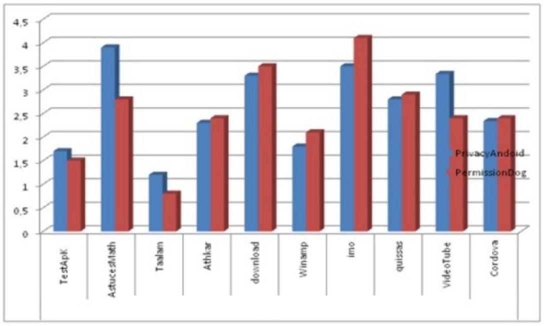


Fig. 6. Galaxy tab 4

B. *Discussion*

We conducted an experimental study on a set of 10 applications installed upon 5 Android mobile devices. Applications have scores that vary between 0.4 and 5. This score quantifies the risk toward privacy. The more the score is high, the more the application is dangerous for users' privacy. We note that the scores of applications vary for to the different mobile devices. For instance, results for the Huawei Honor6 device show that AstucesMath application has a score of 5 while for Evertek mobile device it has a score of 3.7. This can be explained by the fact that our proposed model varies dynamically based on its different uses applications and related permissions. The relative importance of permissions is a quantitative parameter that measures the weight of a permission compared to the other permissions installed on the same device. We observe that the results obtained using PrivacyAndroid and PermissionDog are very similar on the different mobile devices. This similarity allows us to conclude that our application succeeds in detecting permissions required by an application and in estimating its risk before its installation. Our proactive approach is as effective as reactive approaches that only estimate the risk of an application after its installation.

VI. 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 of the model are the severity and the relative importance. The severity of permissions and their interactions are estimated with the EBIOS risk assessment method. The determination of the relative importance have been formulated as MCDM problem and solved using the AHP method. In order to validate our proactive approach, we compared its results with those of a reactive approach. For this purpose, we calculated the scores of different applications on several mobile devices. We performed the calculation using our proactive PrivacyAndroid application. Then we did the same, using the

PermissionDog reactive application. We have noticed that the results obtained are close. Thus our application succeeds in detecting the permissions required by an application and to estimate the risk of the latter before its installation. Our approach is as effective as reactive approaches that only estimate the risk of an application after its installation. The contribution of this paper is to identify significant parameters that should be taken into account to assess privacy risk linked to Android permissions. The proposed privacy risk assessment model contributes to enhance the users' awareness of the risk to their privacy. It helps users in the decision making regarding permission granting while taking into account the actual context of the users' device. This would also contribute also to encourage applications developers to seek access to the only required resources and permissions.

REFERENCES

[1] Android Security Overview, 2014, Retrieved 2014, from http://source.android.com/devices/tech/secsecur

[2] Enck, W. et al., Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones, in Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation, Vancouver, BC, Canada, 2010.

[3] 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 and Trustworthy Computing, Vienna, Austria, 2012.

[4] Keng, J.C.J. et al., The Case for Mobile Forensics of Private Data Leaks: Towards Large-Scale User-Oriented Privacy Protection, in Proceedings of the 4th Asia-Pacific Workshop on Systems, Singapore, Singapore, 2013.

[5] Rosen, S. et al., AppProfiler: a flexible method of exposing privacy-related behavior in android applications to end users, in Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy. San Antonio, TX, 2013.

[6] Xu, W. et al., Permlyzer: Analyzing Permission Usage in Android Apps, in Proceedings of the 24th IEEE International Symposium on Software Reliability Engineering, Pasadena, CA, 2013.

[7] Sarma, B.P. et al., Android permissions: a perspective combining risks and benefits, in Proceedings of the 17th ACM symposium on Access Control Models and Technologies, Newark, NJ, 2012.

[8] Wang, W. et al., Exploring Permission-induced Risk in Android Applications for Malicious Application Detection, IEEE Transactions on Information Forensics and Security, 2014, 9(11), pp.1869-1882.

[9] Zhang, Y. et al., Vetting undesirable behaviors in android apps with permission use analysis, in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, Berlin, Germany, 2013.

[10] Kiran, K. et al., Performance And Analysis Of Risk Assessment Methodologies In Information Security, International Journal of Computer Trends and Technology (IJCTT), 2013, 4(10), 3685-3692.

[11] Lonita, D., Current established risk assessment methodologies and tools, Essay (Master), University of Twente, 2013.

[12] Commission Nationale de l'Informatique et des Libertés (CNIL), Methodology for Privacy Risk Management, 2012.

[13] Ghazouani, M. et al., Information Security Risk Assessment - A Practical Approach with a Mathematical Formulation of Risk, International Journal of Computer Applications, 2014, 103(8).

[14] Zhou, R. et al., On the Need of Physical Security for Small Embedded Devices: A Case Study with COMP128-1 Implementations in SIM Cards, 2013, Retrieved 2015, from http://fc13.ifca.ai/slide/4-3.pdf

[15] Castellucia, C., GSM security, Retrieved 2015, from http://planete.inrialpes.fr/~ccastel/COURS/gsm.pdf

[16] Fudan, J.G. et al., Interaction Effects of Contextual Cues on Privacy Concerns: The Case of Android Applications, System Sciences (HICSS), 2015, pp.3498-3507.

[17] Android permissions explained, security tips, and avoiding malware, 2015, Retrieved 2015, from http://androidforums.com/threads/android-permissions-explained-security-tips-and-avoiding-malware.36936/

[18] Blum, S. App Permissions Explained - What Do They Really Mean?, 2012, Retrieved 2015, from https://www.androidpit.com/app-permissions-explained

[19] Ahmed, N., Use Permissions to Secure Your Private Data from Android Apps, 2013, Retrieved 2015, from http://techpp.com/2010/07/30/android-apps-permissions-secure-private-data/

[20] 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.

[21] Saaty, T.L., Decision making with the analytic hierarchy process, International journal of services sciences, 2008, 1(1), pp.83-98.

[22] Melvin, A., Decision-Making using the Analytic Hierarchy Process (AHP) and SAS/IML, Southeast SAS Users Group (SESUG), Durham, North Carolina, 2012.

[23] Ben Yahia, S. et al., Frequent closed itemset based algorithms: a thorough structural and analytical survey, ACM SIGKDD Explorations Newsletter, 2006, 8(1), pp. 93-104.

[24] 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.

[25] Mylonas, A., et al., Delegate the smartphone user? Security awareness in smartphone platforms, Computers & Security, 2013, pp.47-66.

[26] Google: Privacy policies for android apps developed by third parties 2013, Retrieved 2016, from https:// support.google.com/googleplay/answer/2666094?hl=en

[27] Theoharidou, M., Mylonas, A. and Gritzalis, D., A risk assessment method for smartphones, in Proceedings of Information security and privacy research, 2012, pp. 443-456.

[28] Mylonas, A., Theoharidou, M. and Gritzalis, D., Assessing privacy risks in android: A user-centric approach, in Proceedings of Risk Assessment and Risk-Driven Testing, 2013, pp.21-37.

[29] Kiran, K. et al., Performance And Analysis Of Risk Assessment Methodologies In Information Security, International Journal of Computer Trends and Technology (IJCTT), 2013, 4(10), pp.3685-3692.

[30] IBM SPSS Statistics, Retrieved 2016, from https://www.ibm.com/marketplace/cloud/statistical-analysis-and-reporting/us/en-us

[31] PermissionDog, Retrieved 2016, from https://play.google.com/store/apps/details?id=com.PermissioDog&hl=fr

[32] Hamed, A., Kaffel-Ben Ayed, H., Privacy Risk Assessment and Users' Awareness for Mobile Apps Permissions, accepted at the 13th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA 16), November 2016, Agadir, Morocco.