Beacon Alarming: Informed Decision-Making Supporter and Privacy Risk Analyser in Smartphone Applications

Majid Hatamian*, Jetzabel Serna-Olvera*
*Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe University of Frankfurt
Frankfurt am Main, Germany
E-mail: majid.hatamian.h@ieee.org, jetzabel.serna@m-chair.de

***Abstract*—We are currently confronting with a large number of Smartphone applications, which are developed for different purposes that on the one hand, may benefit users by easing many of their daily tasks, while on the other hand, may threaten their privacy. An important issue regarding this situation is that, smartphone users are often unaware of the privacy risks or even of the data collected by applications running on their devices. For this reason, it is an essential need to make the users aware of the potential misuses as well as the associated privacy risk consequences. In this paper, we introduce a novel approach called Beacon Alarming. Beacon alarming is introduced as a monitoring and permission manager framework to enhance the users awareness of data gathered by their installed applications. We further expand the functionality of our proposed beacon alarming system by employing fuzzy logic in order to assess the privacy risk score of each of the installed applications taking into consideration the information obtained from beacon alarming module. Accordingly, this innovative method enables users to make more logical and informed decisions.**

***Index Terms*—smartphone applications; privacy; usability; beacon alarming; privacy risk score; fuzzy logic.**

I. Introduction

With the rapid growth of technology, our life is now significantly surrounded by or even dependent on the use of smartphones. Similarly, the number of mobile applications available has exploded over the past few years. For instance, the number of available applications in the Google Play Store surpassed 1 million applications in July 2013 and was most recently placed at 2.4 million applications in September 2016. At the same time, the number of cumulative applications which were downloaded from the Google Play app store reached by 15 million from 50 to 65 million between July 2013 and May 2016 [1], [2]. However, while smartphone apps provide tremendous benefits to users, especially in terms of personalized and context-sensitive services; having access to a multiplicity of sensitive resources also poses a series of privacy and security risks. Security and privacy have always been a serious concern in the field of information technology [3], [4]. Privacy is an extensive concept that captures various aspects of our life and, therefore, several definitions of privacy exist. In the information security context 'privacy' usually refers to the expectation and rights that people have concerning their personal information in order to securely and adequately handle this information [5], [6]. In this regard, current smartphone ecosystems reflect a fundamental tension between privacy and usability. The more smartphone apps need to provide usability, the more they require to have access to data [7]. Above all, users are often unaware of the data collected by their applications. Accordingly, they express discomfort once they realise that their data are being collected without their consent [8].

In order to address the aforementioned issue, the most common approach for preserving privacy is to give the ability to the users to evaluate the permissions requested by an application and determine whether they feel comfortable granting it or not. In fact, in such solutions a privacy control approach is prepared for Android to enable selectively granting, denying or confining access to specific permissions on a certain application. However, it has been demonstrated that these approaches cannot efficiently operate [9], [10]. Especially, since many users do not understand the implications of their decisions. In fact, permission granting approach can be confusing for users because they usually pay limited attention to permission screens and have poor understanding of what the permissions mention. On the other hand, several works have been proposed to extract the privacy risk from metadata on smartphone ecosystems, including user comments, ratings, application descriptions, etc. One fundamental constraint is that this kind of information is inexpressive and sometimes fails to support a fine-grained measurement about how and to which extent the data are being accessed.

Our Work: The main contributions of this work can be summarised as follows:

- Performing an in-depth log analysis to extensively analyse and check the permissions that are being accessed by each installed application
- Providing a tool to effectively inform the users of the data which are being accessed by different installed applications
- Proposing an intelligent approach by benefiting from fuzzy logic to measure the privacy risk score of the applications

The rest of this paper is organized as follows. In Section II we generally explain the different parts of proposed method. In Section III, we introduce our approach for log analysis and beacon alarming system with their respective modules. In Section IV, we explain the steps which should be taken into account to measure the privacy risk score. This section also describes how fuzzy logic can be used as a decision-making method to intelligently estimate the privacy risk score. Finally, we discuss the future work and conclude the paper in Section V.

II. Propose Method

In this section we propose an informed decision-making supporter to effectively inform the users of the level to which the data are accessed. Consequently, this continuously precaution which owes to the beacon alarming concept, plays a crucial role in acting against privacy-invasive applications.

The proposed beacon alarming is aimed to effectively inform the users of the data which are being accessed by different installed applications. As a result, it is supposed to increase the users' awareness of the collected data by their applications. Due to the fact that, we design and implement an innovative GUI which is expected to attract the users' attention. We further make our approach more intelligent by benefiting from fuzzy logic to measure the privacy risk score of the installed applications. Two inputs are applied to the fuzzy inference system (FIS) to estimate the privacy risk scores. Moreover, we evaluate the privacy risk score with regards to the output of FIS. We measure the privacy risk score regarding a combination of the log analysis, and the sensitivity of the data (which will be described later). More clearly, beacon alarming mechanism has been initiated to monitor different accesses to the permissions, and then, notify users to revise/adjust their application permissions. As a result, the users will be able to more efficiently control their privacy and make more informed decisions. More specifically, by using beacon alarms, users are able to figure out how often and which of their sensitive data are being accessed. Ultimately, they can revamp/restrict their permissions. Figure 1 illustrates the main structure of the proposed method.

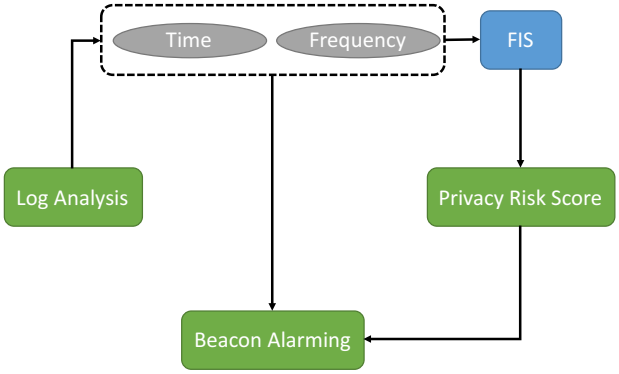


Figure 1: The main structure of the proposed method.

III. Logs Analysis and Beacon Alarming

This section describes how the analysis of data accesses done by each installed application is performed. Consecutively, we introduce the beacon alarming and its corresponding modules.

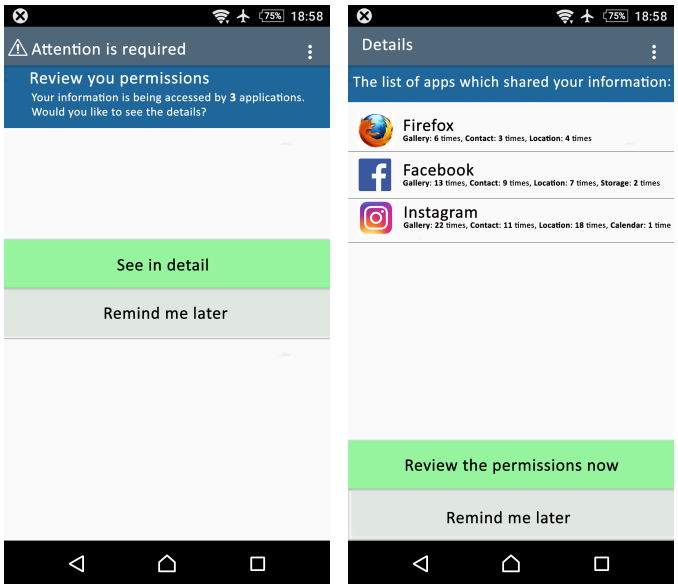
In recent years, a privacy manager tool called AppOps was introduced in Android 4.3. However, in later versions of Android (i.e. Android 4.4.2 and later versions) this tool was made inaccessible unless the mobile device was rooted [11]. However, in our work, we identified that the root access is only needed to access the AppOps management system, e.g. to tell the system to deny access to one of the operations that is controlled by AppOps. As a result, we found that in order to view the AppOps logs, there is no need to root the device, and they are accessible to any application with debugging privileges. Meanwhile, a new permission manager system has been included in Android 6.0 Marshmallow. This new permission manager system is capable of revoking/granting permissions from any application - even ones designed for old versions of Android. Having considering this fact, and, after having done a log analysis concerning the number of accesses that each application has to the data and permissions, we were able to inform the user (by designing a novel alarming mechanism which will be described later) to revise/adjust her permission by benefiting from this new added permission manager system. In what follows, we describe how the log analysis is performed.

In order to collect the logs, a timer is sent to the *PermissionUsageLogger* service periodically. When it is received, the logger queries the AppOps service that is already running on the phone for a list of applications that have used any of the operations we are interested in tracking. We then check through that list and for any application that has used an operation more recently than we have previously seen for it, we store the time at which that operation was used in our own internal log. These timestamps can then be counted to obtain a usage count.

We describe *Beacon Alarming* as an innovative concept to help users to make more rational decisions. To be more clear, beacons are defined as notifications which do not confine selection. In fact, they try to inform users of how they can logically make an informed decision. Once a user receives the beacon alarm, she can revise/adjust her application permissions. It is worth mentioning that in this paper we are trying to behaviourally analyse the installed applications. This is due to the fact that, our goal is to amend the awareness of misconduct behaviours and accessing to sensitive data.

Now, everything boils down to this question of: how can we concentrate the user's attention? From a psychological point of view, the beacon alarming system should be able to

attract the user's attention. For this purpose, we implement a beacon alarming interface in which we report the users about the permissions which are currently being accessed by every installed application, and then, we ask the user to revise (review) her application permissions. The more simpler and clearer the design is, the more efficient and effective the beacon alarming is. Figure 2 shows the proposed beacon alarming interface.



(a) (b)

Figure 2: the proposed beacon alarming interface (a) the notification, (b) the details.

As it can be seen in Fig. 2(a), the user is notified by the beacon alarming notification. The interface of this alarming structure is totally persuasive for the user because:

- there is an attention sentence (with icon)
- it is relatively designed similar to Google permission system (in terms of colors, fonts, etc.)
- the sentences "Review your permission" and "Your information is being accessed by X applications. Would like to see the details?" are aimed to attract the user's attention.

Additionally, Fig. 2(b) demonstrates the details of accessing to sensitive information. These details are shown with respect to the application's name, and the number of applications accessing different types of permissions in a given period.

IV. Privacy Risk Score Measurement

In this section, we suggest a fuzzy inference system to further ameliorate our proposed beacon alarming system which was explained in the previous section. In fact, after doing an in-depth log analysis, and informing the user of the permissions which are being accessed, we aim to propose a fuzzy approach to clarify to what extent an application can be actually harmful for the users' privacy. As a matter of fact, we intend to use fuzzy logic as an upper-level alarming system which makes beacon alarming system more intelligent by measuring the privacy risk score associated to every installed application. Up to know, we did a log analysis and based on it, we proposed a beacon alarming system which is able to inform the user which application has access to which permission. To be more specific, this beacon alarming mechanism clarifies how much users' information is being processed and accessed by different applications which in turn leads to making more informed decisions. Now, we aim to bring in the point of: to which level the accesses that every application has to the permissions can be suspicious and dangerous.

As it was previously mentioned, we aim to use fuzzy logic on top of our proposed beacon alarming system to estimate the privacy risk score related to each app, and support users to make more informed decisions. Fuzzy approaches are appropriate methods to create decision-making systems which are able to relatively operate and decide like human beings. The output of a fuzzy controller is obtained from fuzzification of both input(s) and output(s) using the associated membership functions. A crisp input will be converted into different members of the associated membership functions based on its value. As a result, the output of a fuzzy logic controller is based on its memberships of the different membership functions [12], [13].

We suggest to use two inputs for FIS to evaluate and assess the potential risk which may be imposed on the users' privacy, including *time-sensitive permissions* and *frequency-sensitive permissions*. That is to say, we categorize all the permissions into time and frequency. The main idea behind this categorization is that, in a smartphone, some information flows are sensitive to the number of accesses (time). By contrast, the others are sensitive to the quantity of these accesses (frequency).

Additionally, we define two threat levels including *normal* and *dangerous* for managing data access permissions with regards to the beacon alarming. We classify data access to the permissions which are sensitive to time parameter in dangerous category. Similarly, data access to the permissions which are sensitive to frequency parameter is classified in normal category. This is due to the fact that, having access to some permissions (such as Phone Number) is critically dependent upon the time parameter (i.e. one access is sufficient to disclose the Phone Number). In addition, we also categorize some of the permissions (e.g. Location) in dangerous category. In fact, we can define a threshold level, and if accessing to such permissions reaches this threshold, we assort that access as dangerous (not normal).

To measure the privacy risk score regarding the applied inputs to the FIS, the fuzzy output must be defuzzified. In other words, the output of FIS determines the privacy risk score of each application. It is evident that the privacy risk score is introduced as the privacy level of an application. Therefore, privacy risk scores are basically obtained by the data access permissions of a certain application. As a result, our goal is to check each of the dangerous permissions which are requested

by different applications (according to the information which are obtained from beacon alarming system, such as the number of accesses and/or the kind of permission which is whether normal or dangerous). For the sake of convenience, we define a privacy risk score function which is described as follows:

$$F = \sum_{i} \alpha(w_i, f_i),\ \forall f_i \in \{p, f, b\} \quad (1)$$

where p, f, and b are defined as the fitness parameters for F, and they indicate the kind of permission, fuzzy variables, and the number of beacon alarms, respectively. In other words, F is a function of all the above fitness parameters. It is also possible to initially assign arbitrary weights w_i to the fitness parameters.

Algorithm 1 shows the procedure of the proposed method for measuring the privacy risk score.

Algorithm 1 Pseudo-code for measuring the privacy risk score

1. **Procedure**
2. **START**
3. **for** $i = 1; i <= n; i++;$
4. *Calculate* b_i
5. *Determine the type of information flow*
6. *Distinguish the sensitivity of the permissions regarding the fuzzy variables*
7. *if* $b_i < threshold$
8. *then it is not suspicious*
9. *else the threat level is "dangerous"*
10. *Calculate privacy risk score function*
11. *Update the weight* w_i
13. **END for**
14. **END**

V. Conclusion and Future Work

In this paper, we proposed beacon alarming, a novel log monitoring system to support privacy protection in smartphones. Since privacy plays a critical role in smartphone applications, it is an essential necessity to provide an efficient privacy protection solution and make it more persuasive for the users. To this end, we introduced beacon alarming as a novel concept to make the users aware of how they can logically make an informed decision. As soon as the users receive the beacon alarm, they can revise/adjust their application permissions. In the designing of this beacon alarming system, we highlighted the importance of attracting the user's attention as means of better privacy indicators. Furthermore, our approach estimates a privacy risk score of an application with regards to a combination of beacon alarms and fuzzy logic. With this measurement, we intended to distinguish the anomalous permission requests done by different applications. As a consequence, users will be able to detect applications with anomalous behaviour.

There are some practical and theoretical issues that need to be addressed, however. On the practical side, the threat levels, as represented and supported by the assumptions, should be extended. As well as, the beacons should be diffused more intelligently to avoid the feeling of discomfort if the users receive too many of them. On the theoretical side, the analysis of the privacy risk score is rather informal. Much remains to be done in this regard, especially when comparing to the complexity of existing risk assessment approaches. Also, there is a possibility to initially assign arbitrary weights to the different fitness parameters. This might further increase the functionality of the privacy risk score analyser.

VI. Acknowledgement

This research work has received funding from the H2020 Marie Sklodowska-Curie EU project "Privacy&Us" under the grant agreement No 675730.

References

[1] "Number of available applications in the Google Play Store from December 2009 to February 2016," accessed September 29, 2016, http://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

[2] "Cumulative number of apps downloaded from the Google Play as of May 2016 (in billions)," accessed September 29, 2016, http://www.statista.com/statistics/281106/number-of-android-app-downloads-from-google-play/

[3] R. Turn, and W. H. Ware, *Privacy and security issues in information systems*. RAND Corporation, 1976.

[4] A. Naghizadeh, B. Razeghi, E. Meamari, M. Hatamian, and R. E. Atani, "C-trust: A trust management system to improve fairness on circular P2P networks," Peer-to-Peer Networking and Applications, vol. 9, no. 6, pp. 1128–1144, 2016.

[5] M. E. Whitman, and H. J. Mattord, "Principles of information security," *Boston, Mass.: Thomson Course Technology*, 2003. Print.

[6] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," in *Proceedings of the* 8^{th} *ACM Symposium on Usable Privacy and Security*, China, pp. 1–16, 2012.

[7] P. Gerber, M. Volkamer, and K. Renaud, "Usability versus privacy instead of usable privacy: Googles balancing act between usability and privacy," ACM SIGCAS Computers and Society, vol. 45, no. 1, pp. 116–21, 2015.

[8] M. Nauman, S. Khan, and X. Zhang, "Reconciling mobile app privacy and usability on smartphones: could user privacy profiles help?," in *Proceedings of the* 23^{th} *International Conference on World Wide Web*, China, pp. 201–212, 2014.

[9] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "A conundrum of permissions: installing applications on an android smartphone," in *Proceedings of the* 16^{th} *International Conference on Financial Cryptography and Data Security*, Bonaire, pp. 68–79, 2012.

[10] M. Nauman, S. Khan, and X. Zhang, "Apex: Extending android permission model and enforcement with user-defined runtime constraints," in *Proceedings of the* 5^{th} *ACM Symposium on Information, Computer and Communications Security*, China, pp. 328–332, 2010.

[11] "Google removes vital privacy feature from Android, claiming its release was accidental," accessed July 17, 2016, https://www.eff.org/deeplinks/2013/12/google-removes-vital-privacy-features-android-shortly-after-adding-them/

[12] L. A. Zadeh, "Fuzzy sets," Information and Control, vol. 8, pp. 338–353, 1965.

[13] M. Hatamian, M. A. Bardmily, M. Asadboland, M. Hatamian, and H. Barati, "Congestion-aware routing and fuzzy-based rate controller for wireless sensor networks," Radioengineering, vol. 25, no. 1, pp. 114–123, 2016.