A Curious Case of "Consent Button"

Neither do I want to accept nor decline

Nurul Momen
Karlstad University
nurul.momen@kau.se

Lothar Fritsch
Karlstad University
lothar.fritsch@kau.se

1. INTRODUCTION

Smartphone apps have become an integral part of todays' society. Apps are able to collect, process and transmit information about individuals which raises serious privacy concerns. Our collaborative research is focused on determining apps' resource access patterns and its' potential impact on user privacy [3, 4, 6–8, 11]. As the user struggle to perceive actual intention of apps and potential implication on privacy, we aim at developing Transparency Enhancing Tools (TETs) that come with computational cost, overhead and storage complexity. We developed prototypes and modules that can provide privacy impact assessment cues. However, it is difficult for the user to take privacy-preserving decisions with ease. In this talk, we would like to present some of the cues, preliminary results, discuss promising paths to explore (i.e. evaluation of consent given earlier) and seek feedback from the audience.

2. PRIVACY IMPACT ASSESSMENT CUES

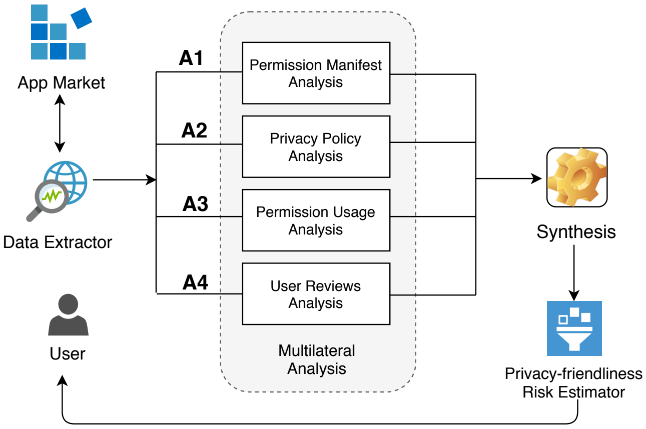

Figure 1: Determining privacy friendliness of fitness apps through multilateral analyis of their privacy policies, permission requests, idle-time resource access and threat counts from user reviews [5].

Which privacy-sensitive data does a mobile app really aim to extract from smartphones? Does the app behavior correlate with the promises of the privacy policy? What are the user's privacy-invasive experiences with the apps? Do the user's concerns reflect correlated privacy threats? And how will a consumer or a public authority decide which app of a set of possible candidates poses the least or an acceptable privacy risk and impact on its users? To answer these questions, we develop a method that extracts data about apps from several sources and prepares the data to enable comparison of app privacy impact. The method uses four data sources. We demonstrate the use of the method with a case study performed on ten popular fitness and exercise apps available on the Android app market. Our multilateral methodology allows the assessment and comparison of privacy implication of an app from four different perspectives: a) comparison of apps' resource requirement, b) assessment of those requirements based on their corresponding privacy policies, c) quantification of their permission access efforts during run-time and d) assessment of privacy concerns raised by users. We combine ex-post and ex-ante transparency perspectives and present the overlaying results in tabular and graphical overlays as well as in an aggregated privacy impact score which can offer an overview of privacy consequences for a given set of apps. This ranking enables sorting the apps by their potential privacy impact. Figure 1 depicts the overall architecture of our approach. The case study, focused on popular fitness apps, found considerable gaps between the privacy policies and the privilege requests and in addition, documented suspicious app behavior of some of the apps in the app set. We intend to present some of the highlights of our findings.

3. USING ASSESSMENT CUES

A subset of the aforementioned cues are used in another study to identify behavioral changes over long period of time. In order to measure apps' data access pattern, we collected meta data months before General Data Protection Regulation (GDPR) came into effect [2]. Recently, we repeated the data collection campaign which allowed us to compare and highlight the changes in app behavior due to regulatory shift. Our study focuses on the apps' use of permission privileges through the Android operating systems' permissions mechanism. We focused on the so-called dangerous permissions[1]– a group of access privileges defined as sensitive by Android developers as they may have effect on the users' sensitive data- that regulate access to location, contacts, phone log, sensors and other data sources. We monitored app permission access request data in March 2017. To compare, we installed a subset of the post-GDPR version of the respective apps in December 2018 and ran a one-week data collection campaign. The data collection was done with the

[1] `https://developer.android.com/guide/topics/permissions/overview#dangerous_permissions`

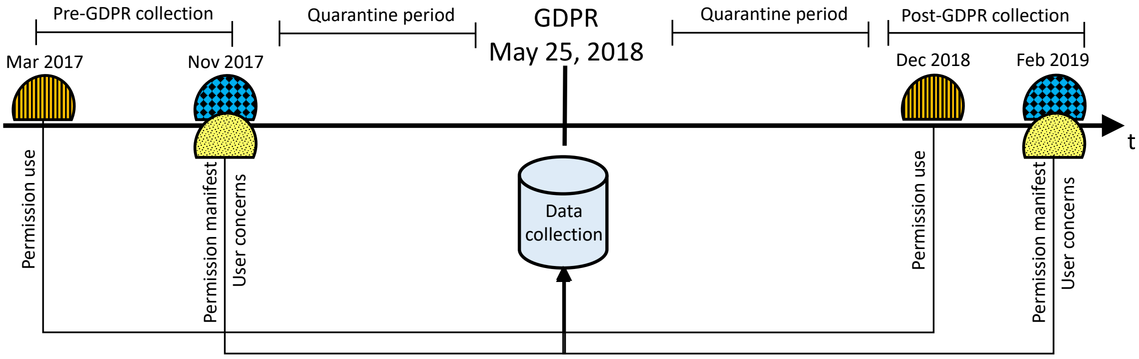

Figure 2: Overview of data collection periods. Data was collected with an approximate 6-month quarantine before and after GDPR implementation. App manifest and user concerns were collected after app permission use profiling. Quarantining ensured that app producers had time to adapt apps to GDPR between the to collection periods [10].

A-ware data capture app described in [9,11] and the data is stored in an on-line collection database [1]. Figure 2 shows how the data collection was organized.

In our data, we have observed changes in app behavior and in user feedback that point towards positive impact of the GDPR on apps. The number of permissions demanded in app manifestos has somewhat declined, strongest in the weather app group. Idle apps seem to use fewer number of permissions than they are actually prepared to use, with observed reduction in permission use. In user feedback, a moderate decline in concerns related to privacy can be seen, though worries for targeted advertising seem to have increased.

4. CONCLUSION

We would like to cover three major aspects in our intended talk: a) introducing a multilateral method, consisting of four different impact parameters, to measure apps' privacy-friendliness, and presenting the priliminary results from a case study which was conducted by applying this method, b) presenting results from a long-term data collection campaign through the lens of this method which highlights app behavior changes due to GDPR, and c) our thoughts on utilizing these impact assessment cues to re-evaluate decisions taken earlier which could support better intervenability. Lastly, we would like to seek feedback from the audience regarding feasibility and usability of our method, parameters, cues and findings, which would allow us to tune some parameters for future work.

5. REFERENCES

[1] A. Carlsson, C. Pedersen, F. Persson, and G. Söderlund. Kaudroid: A tool that will spy on applications and how they spy on their users. Technical report, Karlstad University, Department of Mathematics and Computer Science, 2018.

[2] EU Regulation. 679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Off J Eur Union*, page L119, 2016.

[3] L. Fritsch and N. Momen. Derived partial identities generated from app permissions. In *Open Identity Summit (OID) 2017*. Gesellschaft für Informatik, 2017.

[4] M. Hatamian, A. Kitkowska, J. Korunovska, and S. Kirrane. "it's shocking¡': Analysing the impact and reactions to the a3: Android apps behaviour analyser. In F. Kerschbaum and S. Paraboschi, editors, *Data and Applications Security and Privacy XXXII*, pages 198–215, Cham, 2018. Springer International Publishing.

[5] M. Hatamian, N. Momen, L. Fritsch, and K. Rannenberg. A Multilateral Privacy Impact Analysis Method for Android Apps. *accepted for publication in 2019.*

[6] M. Hatamian, J. Serna, and K. Rannenberg. Revealing the unrevealed: Mining smartphone users privacy perception on app markets. *Computers & Security*, 2019.

[7] M. Hatamian, J. Serna, K. Rannenberg, and B. Igler. Fair: Fuzzy alarming index rule for privacy analysis in smartphone apps. In J. Lopez, S. Fischer-Hübner, and C. Lambrinoudakis, editors, *Trust, Privacy and Security in Digital Business*, pages 3–18, Cham, 2017. Springer International Publishing.

[8] M. Hatamian and J. Serna-Olvera. Beacon alarming: Informed decision-making supporter and privacy risk analyser in smartphone applications. In *To be appeared in the Proceedings of the* 35th *IEEE International Conference on Consumer Electronics (ICCE), USA*, 2017.

[9] N. Momen. Towards measuring apps' privacy-friendliness (licentiate dissertation). Technical Report 2018:31, Karlstad University, Department of Mathematics and Computer Science, 2018.

[10] N. Momen, M. Hatamian, and L. Fritsch. Did app privacy improve after GDPR? *accepted for publication in 2019.*

[11] N. Momen, T. Pulls, L. Fritsch, and S. Lindskog. How much privilege does an app need? investigating resource usage of android apps (short paper). In *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, pages 268–2685, Aug 2017.