 doi:10.20944/preprints202007.0330.v1

Article

Data privacy management in public environments

Hugo Lopes [1], Valderi R. Q. Leithardt [1,4,5,*], Ivan Miguel Pires [2,3], Raúl García-Ovejero [6] and María Navarro-Cáceres [6,]

[1] Computer Science Department, Universidade da Beira Interior, 6201-001 Covilhã, Portugal; lopeshma@gmail.com (H.L.);
[2] Instituto de Telecomunicações, Universidade da Beira Interior, 6201-001 Covilhã, Portugal; impires@it.ubi.pt (I.M.P.)
[3] Computer Science Department, Polytechnic Institute of Viseu, 3504-510 Viseu, Portugal
[4] Laboratório de Sistemas Embarcados e Distribuídos (LEDS), Programa de Mestrado em Computação Aplicada (MCA), Universidade do Vale do Itajaí – Univali, Brasil; valderi@univali.br (V.L.)
[5] COPELABS, Universidade Lusófona de Humanidades e Tecnologias, Lisboa, Portugal.
[6] Expert Systems and Applications Lab, Faculty of Science, University of Salamanca, Plaza de los caídos s/n, 37008 Salamanca, Spain; raulovej@usal.es (R.G.-O), maria90@usal.es (M.N.-C.);
* Correspondence: valderi.leithardt@ubi.pt: (V.L.)

Abstract: The mobile devices caused a constant struggle for the pursuit of data privacy. Nowadays, it appears that the number of mobile devices in the world is increasing. With this increase and technological evolution, thousands of data associated with everyone are generated and stored remotely. Thus, the topic of data privacy is highlighted in several areas. There is a need for control and management of data in circulation inherent to this theme. This article presents an approach of the interaction between the individual and the public environment, where this interaction will determine the access to information. This analysis was based on a data privacy management model in public environments created after reading and analyzing the current technologies. A mobile application based on location via Global Positioning System (GPS) was created to substantiate this model, which it considers the General Data Protection Regulation (GDPR) to control and manage access to the data of each individual.

Keywords: Data Privacy; Mobile devices; Environment Privacy; General Data Protection Regulation (GDPR).

1. Introduction

Mobile devices are increasingly present in the daily lives of each individual, and they considered it essential for their daily activities. Each machine is a source of private information about the individual who owns it and who surrounds it. As these data are considered to belong to the individual, collection and treatment cannot be carried out without the consent of the individual. Based on this assumption, the processing and collection of private data in a non-consensual way, damages and violates your privacy and may cause damage to it [1]. The sharing of any data depends on the individual's perception and willingness to share such private data, respecting the privacy preferences of each individual, which is the primary motivation of the study [1].

As a primary objective, a data privacy management model was created in public environments based on the comparison and study of state of the art in and considering the comparison of existing solutions. After this comparison, the mobile application representing the public data management and privacy model will be presented.

The proposed model contributes to the analysis of all environmental situations with the technology involved, and it guarantees a correct treatment of their data.

This paragraph ends the introduction. Section 2 presents the background of the proposed solution. The materials are presented in section 3, showing the requirements in section 4. Next, Section 5 offers the details about the implementation. The validation of the solution was introduced

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2020 doi:10.20944/preprints202007.0330.v1

in section 6. Finally, the discussion of the results is presented in section 7, ending with the conclusions in section 8.

2. Background

Data privacy has had a vast prominence in society. Several approaches are taken to realize the dream of one day. There could be a world in which there is a real state of privacy for the individual. For such privacy to exist, it is necessary to take into account aspects such as the individual's behaviour, existing technologies, political, economic and social limits [2]. Mobile devices are one of the most significant sources of information about each individual, as they reflect habits, tastes and characteristics related to each one. Considering that mobile devices have such data, there is a need to control and manage how this dissemination is done [1].

2.1. Comparison with prior work

For the elaboration of the privacy management model in public environments, we analyzed the related work developed between 2017 and 2020. The related works examined were:

- State of the art on Privacy Risk Estimation Related to Android Applications [3];
- Introducing Privacy in Screen Event Frequency Analysis for Android Apps [4];
- Privacy Risk Analysis and Mitigation of Analytics Libraries in the Android Ecosystem [5];
- Analyzing Android App Privacy with GP-PP Model [6];
- GUILeak: Tracing Privacy Policy Claims on User Input Data for Android Applications [7];
- IoT Big Data Security and Privacy Versus Innovation [2];
- PAU: Privacy Assessment method with Uncertain Consideration for cloud-based vehicular networks [8];
- UbiPri – Middleware para Controle e Gerenciamento de Privacidade em Ambientes Ubíquos [9].

A comparison was obtained between the model performed and the related works considered. In Table 1, we can see that the related works are related to data privacy considering the following approaches, such as user, application, generalized environment and public environment. Thus, the following definitions will be found:

- Address: the work addresses the requirement addressed;
- Not address: the work does not address the requirement;
- Not described: No information was found about the requirement addressed;
- Under Development: The requirement is still under development. It is usually pointed out frequently in tests, validations, results obtained or future work.

Table 1. Relation between data privacy approaches and the different studies.

Study:	**Data Privacy Approaches:**			
	User:	**Application:**	**Generalized environment:**	**Public environments:**
May *et al.* [3]	Address	Address	Not described	Not described
Zhang *et al.* [4]	Address	Address	Not described	Not described
Liu *et al.* [5]	Address	Address	Not described	Not described
Kesswani *et al.* [6]	Address	Address	Not described	Not described
Wang *et al.* [7]	Address	Not address	Not described	Not described
Sollins *et al.* [2]	Address	Not address	Address	Not described
Feng *et al.* [8]	Not described	Address	Not described	Not described
Leithardt *et al.* [9]	Address	Address	Address	Not address
This study	Address	Address	Address	Address

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2020 doi:10.20944/preprints202007.0330.v1

After comparison, we can verify the approaches considered about the data privacy, where the authors' focus was centred on the user and the application. On the other hand, concerning the specific public environment, previous works do not describe or address the theme, so we can verify that the work elaborated has this aspect as its main contribution.

2.2. Comparison with other solutions

The following solutions were analyzed to understand its relation to the subject of this analysis:

- MoveWithMe [10];
- Priser [11];
- ShiftRoute [12];
- SieveDroid [13];
- UbiPri [9].

Thus, Table 2 shows the implementation of local privacy, mobile devices, and geolocation in the different solutions available in the literature.

Table 2. Relation between the implemented features and the applications.

Applications:	**Approaches:**		
	Local Privacy:	**Mobile devices:**	**Geolocation:**
MoveWithMe [10]	Yes	Yes	Yes
Priser [11]	Yes	Yes	Yes
ShiftRoute [12]	Yes	Yes	Yes
SieveDroid [13]	No	Yes	No
UbiPri [9]	Yes	Yes	Yes
This study	Yes	Yes	Yes

The solutions presented in Figure 2 are distinct between then, but they have the common purpose of contributing to the privacy of users' data. The approach of data privacy in the environment is highlighted in each solution, where these solutions generally use location-based services for mobile devices.

3. Materials

3.1. Definition of management method for privacy in public environments

Based on the comparison of the state-of-the-art related to the literature and existing implemented solutions, a model was developed for the data privacy management in public environments with the definition of the following categories:

- Unrestricted Public Environment: Environment without time restrictions or access control;
- Temporarily Unrestricted Public Environment: Time-restricted environment without access control;
- Public Environment of Semi-Restricted Access: Environment without time restriction but with access control;
- Public Restricted Access Environment: Time-restricted environment with access control.

Table 3 presents some examples of public environments related to different categories that are generally attributed. The assignment of a category to a given environment depends on legal factors and rules inherent to it.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2020 doi:10.20944/preprints202007.0330.v1

Table 3. Relation between types and environment categories.

Categories:	Public Environments:			
	Unrestricted Public Environment:	**Temporarily Unrestricted Public Environment:**	**Public Environment of Semi-Restricted Access:**	**Public Restricted Access Environment:**
Garden	Yes	No	No	No
Public highway	Yes	No	No	No
Square	Yes	No	No	No
Shopping centre	No	Yes	No	No
Gallery	No	Yes	No	No
Parking	No	Yes	No	No
Trade point	No	No	No	Yes
Service	No	No	Yes	No
Institution	No	No	No	Yes

3.2. Definition of individual profiles

The proposed model focuses on the interaction between the individual and his/her environment. Thus, the following definitions of individual profiles were considered:

- Levels 1, 2 or 3: The user only has access to the information given by her/his environment;
- Level 4: The Administrator is a user that can access the information provided by the category of his/her environment. This user can also perform operations on the information as well as the users.

Regarding the mentioned profiles, for all of them, it will be the environment to determine the access to information.

3.3. Definition of types of information

A direct relationship was made with the category of the environment to define the types of information that a user can access. Thus, as presented in Table 4, the following levels were defined:

- Level 1: Information given by the Unrestricted environment;
- Level 2: Information provided by the Unrestricted and Temporarily Unrestricted environment;
- Level 3: Information provided by the Unrestricted, Temporarily Unrestricted and Semi-Restricted environment;
- Level 4: Information given by the Unrestricted, Temporarily Unrestricted, Semi-Restricted and Restricted environment.

Table 4. Relation between the access level of information and environment categories.

Categories:	Public Environments:			
	Level 1	**Level 2**	**Level 3**	**Level 4**
Unrestricted	Yes	No	No	No
Temporarily Unrestricted	Yes	Yes	No	No
Semi-Restricted	Yes	Yes	Yes	No
Restricted	Yes	Yes	Yes	Yes

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2020 doi:10.20944/preprints202007.0330.v1

4. Requirements

4.1. Functional Requirements

After authentication, the user will have the possibility to view information, manage users and manage the existing information. Regarding the user management, it also includes the option of managing users. Finally, information management consists of the possibility to manage different information.

The main functional requirements are:

- A user with level 4 or Administrator can manage other users and application data;
- A user from level 1 to 3 can check the application data;
- The data query has access mechanisms by location and time.

4.2. Non-functional requirements

The non-functional requirements are:

- The user must be registered to perform authentication;
- Only a user with level 4 can manage other users, and application data;
- For any user to consult any application data, they will have to authorize the location permission;
- The mobile application requires access to the device's location;
- Installing the application on the mobile device requires 4 Megabytes plus the space of data stored by the mobile application;
- The minimum version of Application Programming Interface (API) for the application is 23, which corresponds to Android version 6.0 (Marshmallow).

5. Implementation

The implementation of the Application Layout was carried out using a purely guiding outline. The implementation decisions were influenced by the different needs, which led to the constant modification of this outline. The main goal was to make operations logical and straightforward. In the implementation of the layout, the Extensible Markup Language (XML) was used, using the Android Studio IDE.

5.1. Registration

It was necessary to create a record where the fields name, password, description and a profile level (from level 1 to 4) are filled into the user to have access control to the login application. When an attempt is made to register a user, in turn, the fields are checked before being entered in the local database, to ensure that there are no repeated users. The methods used for this purpose are called insertData and addData. The first is in the activity that controls the DataBaseHelper Database, while the second is in the Registration activity, called RegisterActivity. In the RegisterActivity, it is also possible to edit or delete users. The updateData and updateUser functions are used to modify the user's data. The first is in the RegisterActivity activity and the second in the DataBaseHelper. Finally, to be able to delete a user, the functions deleteData and deleteUser are used. The first is found in the class assigned to the registration of the user RegisterActivity and the second in the activity DataBaseHelper, aimed at controlling the database.

5.2. Authentication

Regarding the implementation of the authentication process, presented in Figure 1, it includes the verification of the fields introduced when registering the user. This process takes place in the LoginActivity activity. The functions used for this purpose are called checkLogin and validate. The first is in the class that controls the database called DataBaseHelper, while the second is located in the Login activity called LoginActivity.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2020 doi:10.20944/preprints202007.0330.v1

Figure 1. Login screen.

5.3. Data management

In the AdminActivity activity, the users with level 4 can manage other users, insert, edit and remove data in the application and have access to the data query activity. The UserActivity for the remaining levels also allows connection to the activity where the information is contained. When the user enters InformationActivity for the first time and has the GPS turned off, they are asked to be activated. If the user refuses, he is prevented from proceeding and redirected to the previous activity, where he will have to repeat the process. Finally, if the user allows access and the Global Positioning System (GPS) is active, the application will obtain the current location, given by latitude and longitude, thus allowing it to remain in the activity. After getting the location of the device, the application only allows access to the data if the user is within an existing location in the database, at a maximum distance (radius in meters) defined for each location point. If the user checks this condition, considering the category of the environment, he will see different types of data, as visible/invisible buttons, that have been implemented for this purpose. Finally, for each type of information belonging to a specific category of environment, there may be a need to be accessed at a time defined in the application. This check is done using the device's date/time using the Calendar class.

Figure 2 shows the management screen related to the users and information. Next, Figure 3 shows the information retrieved by the mobile application. In figure 3, it is possible to verify that the user was in a Restricted Access category location, approximately, where he/she is ten meters from the point defined by latitude and longitude in the database. Finally, Figure 4 shows the working machine used connected in real-time to the mobile testing device.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2020 doi:10.20944/preprints202007.0330.v1

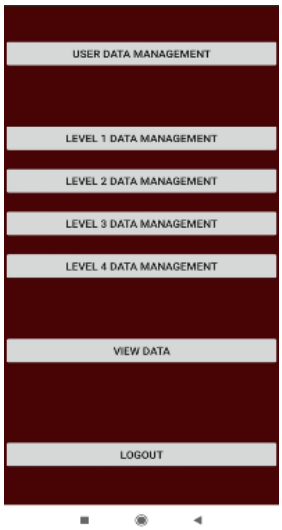

Figure 2. Management of information and users.

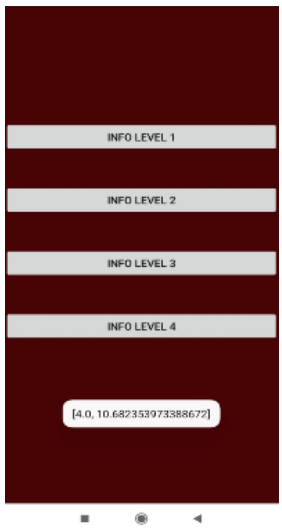

Figure 3. Information retrieved.

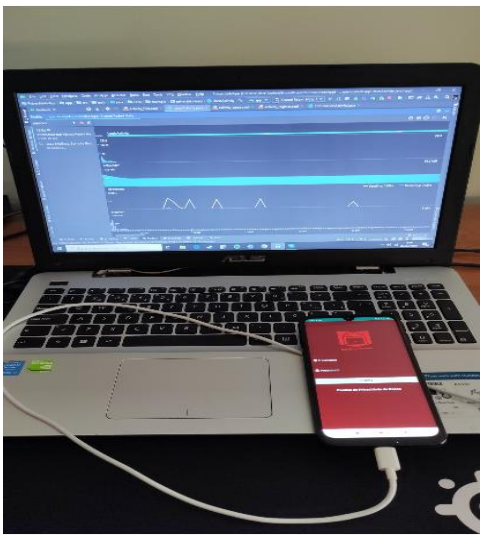

Figure 4. Testing environment of the mobile application.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2020 doi:10.20944/preprints202007.0330.v1

6. Validation

6.1. Test Cases

Some of the application tests were done through real situations in different public environments. For a better understanding, the main tests performed were:

- **Registration/Authentication** ➔ To test the functioning of the user registration/authentication, users with different permission levels were created. In the first attempt to register a new user, the field "name" was placed equal to that of an existing one in the database, and the application prevented registration. In the second attempt to register a new user, the "name" field was placed differently from that of an existing one in the database and the application successfully registered. After the user was introduced, when the authentication attempt was made, a user verification was performed in the database. In the first attempt, the user existed in the database, and the application saved the permission level, so the user was redirected to the activity corresponding to his permission level. In the second attempt, as the user's existence in the database was not verified, he was prevented from entering any activity;
- **Location** ➔ To ensure that the user can only consult the data within a location defined by the application, the coordinates of an "A" location have been inserted away from the device's position and a maximum distance delimited to which it could have been bound. As this distance did not reach the current location of the device, he was not allowed to view any data access button. To test the contrary case, the user walked towards the location "A" defined by the application. As the user walked towards location "A", the application would automatically update its location and check if the place it was in was within the maximum distance from location "A". As there was a match, the buttons became visible, and the corresponding data could be viewed depending on the location's permission. For the tests described above to be possible, first, the application asked for permission to access the device's location, it was refused, and the user was prevented from proceeding and redirected to the previous activity corresponding to his permission level. The same attempt was made again, and when requesting access to the device's location, it was accepted, and the GPS was not active, so he was asked for permission to activate it. The user refused and was immediately prevented from proceeding and redirected to the previous activity where he had to repeat the process previously described until all conditions were met. In the last attempt, the conditions were all checked, and the user managed to remain in the information query activity;
- **Data consultation time** ➔ To ensure that the user could only consult the data at a specific time (day of the week and time), for a particular type of information (information buttons) different consultation times were introduced. The test was done for two different kinds of information, in the first, a consultation time was added outside the time the device was in, the second type of information was within the consultation time imposed by the device. As the first type of information was outside the schedule imposed by the application, it prevented the user from consulting information. Finally, as the second type of data was within the limit imposed by the application, it allowed data to be asked.

6.2. Performance tests

Android Profiler [14] was used to test the application's performance, a tool for monitoring the real-time performance of the application provided by Android Studio [15]. This tool focuses on monitoring the application in the following aspects:

- Energy consumption through the Energy Profiler [16];
- Memory allocation from Memory Profiler [17];
- CPU activity through the CPU Profiler [18];

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2020 doi:10.20944/preprints202007.0330.v1

Figure 5 shows the global chart that evaluates each of the existing components in Android Profiler [14] mentioned above.

Figure 5. General chart of application performance at run time.

The previous figure shows the general chart of performance tests performed on the representative application of the data privacy management model in public environments.

It is possible to see low energy consumption, low processor usage and a small memory allocation.

6. Discussion

Based on the comparison of state of the art referring to Table 1, it can be seen that the elaborated work contributes to an improvement in data privacy since, in addition to making the relationship between the individual and information, it addresses the public environment in which the individual is inserted. In this way, with the categorization carried out, it is possible to determine which are the most critical public environments where there should be a different treatment of the information of each individual. From this categorization, it is also possible to define what type of information will be made available in each environment, thus having a direct relationship between the environment and information. In this way, we will see an improvement in the management of the individual's privacy in public environments. The implementation referring to the chapter where software engineering is described using use case diagrams and activity diagrams has as focus the use of GPS and permission to access the user's location.

From the test scenarios within a set of public environments, it reflects the functioning and response of the application to changes in context. Thus, it is possible to obtain real results on the interaction with the individual.

Finally, we can conclude through tests performed using the Android Profiler tool [14] that satisfactory results were obtained in terms of the use of computational resources and energy consumption.

7. Conclusions

This project consisted of the elaboration of a data privacy management model focused on the public environment, for this purpose a mobile application was created that uses GPS location and device time as a basis to determine access to information in each location.

This model together with other application models related to data privacy can together form a model considered complete that analyzes all situations that occur in the environment in which any technology is inserted and therefore guarantee users a correct treatment of their data.

As the study of this theme reached more significant proportions, there was a need to study the central theme in more depth. Consequently, it was concluded that despite the application functioning

well, issues such as GPS accuracy and energy consumption derived from the use over a long time could limit its operation.

In the future, it would be interesting to make some improvements in terms of precision and energy consumption using Bluetooth Low Energy [11], using a database connected to a server for better treatment, exchange and management of information between the database and the application. In addition to the points mentioned, issues such as application security and the use of Artificial Intelligence algorithms could bring improvements in the operation of the application.

Author Contributions: Conceptualization, methodology, software, validation, formal analysis, investigation, writing—original draft preparation, writing—review, project administration and editing: H.L and V.L, visualization, writing—review and editing: I.M.P., R.G.-O and M.N.-C.

Funding: This work is funded by FCT/MEC through national funds and co-funded by FEDER-PT2020 partnership agreement under the project **UIDB/EEA/50008/2020**. This work was partially supported by Fundação para a Ciência e a Tecnologia under Project **UIDB/04111/2020.**

Acknowledgements: This work is funded by FCT/MEC through national funds and when applicable co-funded by FEDER-PT2020 partnership agreement under the project **UIDB/EEA/50008/2020**. (*Este trabalho é financiado pela FCT/MEC através de fundos nacionais e cofinanciado pelo FEDER, no âmbito do Acordo de Parceria PT2020 no âmbito do projeto UIDB/EEA/50008/2020*). This article is based upon work from COST Action IC1303-AAPELE—Architectures, Algorithms and Protocols for Enhanced Living Environments and COST Action CA16226–SHELD-ON—Indoor living space improvement: Smart Habitat for the Elderly, supported by COST (European Cooperation in Science and Technology). More information in www.cost.eu.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Leithardt, V.R.Q.; Geyer, C.F.R.; Silva, J.M.S. *Controle e gerenciamento de privacidade de dados*; Novas Edições Acadêmicas, 2019; ISBN 978-3-8417-1533-3.
2. Sollins, K.R. IoT Big Data Security and Privacy Versus Innovation. *IEEE Internet Things J.* **2019**, *6*, 1628–1635, doi:10.1109/JIOT.2019.2898113.
3. May, Z.E.; Kaffel Ben Ayed, H.; Machfar, D. State of the art on Privacy Risk Estimation Related to Android Applications. In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC); IEEE: Tangier, Morocco, 2019; pp. 889–894.
4. Zhang, H.; Latif, S.; Bassily, R.; Rountev, A. Introducing Privacy in Screen Event Frequency Analysis for Android Apps. In Proceedings of the 2019 19th International Working Conference on Source Code Analysis and Manipulation (SCAM); IEEE: Cleveland, OH, USA, 2019; pp. 268–279.
5. Liu, X.; Liu, J.; Zhu, S.; Wang, W.; Zhang, X. Privacy Risk Analysis and Mitigation of Analytics Libraries in the Android Ecosystem. *IEEE Trans. on Mobile Comput.* **2020**, *19*, 1184–1199, doi:10.1109/TMC.2019.2903186.
6. Kesswani, N.; Lyu, H.; Zhang, Z. Analyzing Android App Privacy With GP-PP Model. *IEEE Access* **2018**, *6*, 39541–39546, doi:10.1109/ACCESS.2018.2850060.
7. Wang, X.; Qin, X.; Hosseini, M.B.; Slavin, R.; Breaux, T.D.; Niu, J. GUILeak: tracing privacy policy claims on user input data for Android applications. In Proceedings of the Proceedings of the 40th International Conference on Software Engineering; ACM: Gothenburg Sweden, 2018; pp. 37–47.
8. Feng, X.; Wang, L. PAU: Privacy Assessment method with Uncertainty consideration for cloud-based vehicular networks. *Future Generation Computer Systems* **2019**, *96*, 368–375, doi:10.1016/j.future.2019.02.038.
9. Leithardt, V.R.Q. UbiPri : middleware para controle e gerenciamento de privacidade em ambientes ubíquos. *UBiPri : middleware control and privacy management in ubiquitous environments* **2015**.
10. Kang, J.; Steiert, D.; Lin, D.; Fu, Y. MoveWithMe: Location Privacy Preservation for Smartphone Users. *IEEE Trans.Inform.Forensic Secur.* **2020**, *15*, 711–724, doi:10.1109/TIFS.2019.2928205.
11. Silva, L.A.; Valderi R. Q. Leithardt; Rudimar S. Dazzi; Silva, J.S. Priser - Utilização De Ble Para Localização E Notificação Com Base Na Privacidade De Dados. **2018**, doi:10.5281/ZENODO.1336806.
12. Zhang, P.; Hu, C.; Chen, D.; Li, H.; Li, Q. ShiftRoute: Achieving Location Privacy for Map Services on Smartphones. *IEEE Trans. Veh. Technol.* **2018**, *67*, 4527–4538, doi:10.1109/TVT.2018.2791402.
13. Huang, J.; Xiong, Y.; Huang, W.; Xu, C.; Miao, F. SieveDroid: Intercepting Undesirable Private-Data Transmissions in Android Applications. *IEEE Systems Journal* **2020**, *14*, 375–386, doi:10.1109/JSYST.2019.2938611.

 doi:10.20944/preprints202007.0330.v1

14. Medir o desempenho do app com o Android Profiler Available online: https://developer.android.com/studio/profile/android-profiler?hl=pt (accessed on Jul 10, 2020).
15. Android | The platform pushing what's possible Available online: https://www.android.com/ (accessed on Jul 10, 2020).
16. Inspecionar o uso de energia com o Energy Profiler Available online: https://developer.android.com/studio/profile/energy-profiler (accessed on Jul 10, 2020).
17. Ver as alocações de heap e memória do Java com o Memory Profiler Available online: https://developer.android.com/studio/profile/memory-profiler (accessed on Jul 10, 2020).
18. Inspecionar atividades de CPU com o CPU Profiler Available online: https://developer.android.com/studio/profile/cpu-profiler (accessed on Jul 11, 2020).