Towards Improving Privacy Awareness Regarding Apps' Permissions on Linux Based Mobile OS

Nurul Momen[1] and Marta Piekarska[2]

[1] Karlstad University, Sweden (nurul.momen@kau.se)
[2] Technische Universität Berlin, Germany (marta@sec.t-labs.tu-berlin.de)

Abstract Empirical studies show that the flow of personal information through mobile apps has made the device vulnerable in terms of privacy. Cumbersome and inconvenient representation of terms and conditions encourages the user to ignore it and disclose sensitive private information unintentionally. Hence, summarized permissions are presented on mobile devices and users tend to overlook them as well. Rigid structure for using a service and inherited behaviour from desktop applications to accept everything are the reasons behind compelling the user to proceed without paying any attention. Complex permission structure is also a major impediment for consumers that makes it difficult to perceive appropriate consequences of their decisions. We argue that as privacy strongly depends on individual perception, the key to educate and empower the users is to providing them with transparency of what is happening on their smartphones. In consequence we suggest a convenient, transparent and proactive approach to help in understanding and deciding upon privacy implications of apps. We introduce a tool that presents the summary of what applications are installed on a smartphone, which resources they access, and what are the reasons for that. Moreover, the tool is capable of informing the user when certain sensitive data is accessed.

1 Introduction

Smartphones are part and parcel of our daily life: we carry them, store all sorts of personal data on them and even sleep right next to them. Gradually, more and more dimensions are being added to smartphones due to adoption of ubiquitous computing in many sectors. They have become a universal interface for many services operating around us. Significant amount of data is required and collected in order to maintain a real time interaction with the surrounding environment. Additionally, commercial incentives play an important role here. It allows the business entities to offer better services through consumer-centric analysis. A diverse revenue stream is generated by this large data pool for numerous businesses and users are benefited by better product recommendations. However, there is a certain trade-off introduced by giving away personal information - risking individual privacy. As installing an app has become a general solution to many of our problems, it has brought a great deal of privacy concerns. It is indeed necessary to look for smart privacy protection, for example the one that preserves good usability while protecting sensitive data.

As opposed to many other concepts, like computing power, privacy is a topic that is hard to define. The understanding is not only influenced by technical aspects but also by emotions and feelings of individuals which make it difficult to protect. The problem regarding smartphone privacy is two folded - on one side, we need to overcome lack of knowledge, transparency and simplicity; on the other hand, there are the social and psychological aspects. Moreover, depending on the person asked, the tolerance threshold will be different. Also time and context both can play vital roles behind personal preferences. Individual tolerance may fluctuate for same piece of information during variable situations and times.

In general, Linux-based mobile operating systems offer a permission structure for the apps. An app gets access to user data through permissions. Users are asked for their consents in order to proceed with the app. They are also expected to understand the consequences and make informed decisions, which is in fact very unlikely to be right. Though apps require explicit consents from users, no justification is provided. Decisions are being made with misunderstanding and wrong perception about privacy implications, which lead the user to disclose privacy sensitive information unintentionally. It is quite alarming that the user-consent relies on usual bad practice to press *Agree* button after scrolling down the list of permissions.

Our work contributes to the field in the following ways: (1) A theoretical method is proposed for the representation of privacy sensitive data usage on mobile phones which is capable of offering a static and easily adoptable structure; user convenience and ease of understanding are the prime benefits of it, and (2) a tool, named AWARE, is introduced which is implemented on both Firefox OS and Android, to provide convenient, proactive and efficient interface for an overview of personal information usage by installed apps.

The rest of this paper is arranged as follows: a survey was conducted in order to realise the severity of the situation which is described in section 2, the problem is outlined through a discussion of reviewed literature in Section 3. Then solution architecture and implementation strategy are described in Section 4 and 5 respectively. Our prime observations are mentioned in Section 6 and concluding remarks are given in Section 7.

2 Motivation

We conducted an online survey where anyone could participate anonymously. Our intention was to demonstrate the current scenario regarding privacy-unaware user behaviour. Though it was a subjective test and not a controlled group, the result shown in Fig. 1 depicts significant lack of attention from users. The survey took place during the middle of year 2015. Therefore, users are expected to be stranger to the latest runtime permission mechanism of Android. Technical understanding of the participants was not taken into consideration. The summary of our findings is given below:

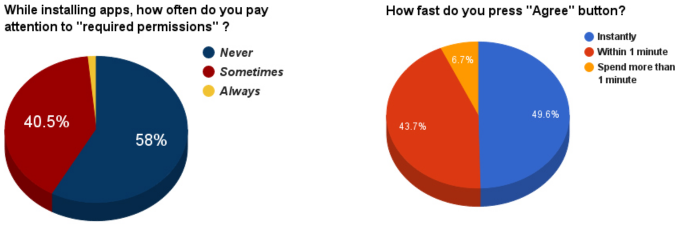


Figure 1: Survey on user behaviour.

- We received **252** responses so far. We asked two questions:
  1. While installing apps, how often do you pay attention to 'required permissions'? Options to answer: Always/Sometimes/Never.
  2. How fast do you press *Agree* button? Options to answer: Instantly/Within one minute/Spend more than one minute.
- We found only 1.6% responses as *Always* for the first question and 93.1% of the responding participants press *Agree* button within one minute or instantly.

Presumably, a significant portion of the survey participants chose 'sometimes' as an answer to the first question. However, the real scenario came out by answering the second question – users hardly spend time to realise the consequences of granting permissions for an app. We can conclusively draw the line here – very few people pay attention to required permissions while installing an app.

3 Related Work

Current research trend is mostly focused on securing and hiding information to meet privacy requirements. There is also an ongoing debate whether to introduce more control to user-interface or not [5,8]. Decision making for important private data based on a cumbersome method could result into a complete rejection from the subscribers [6]. Additionally, there are hurdles to overcome that are caused by absence of proper attention and transparency regarding consequences [2]. Misunderstanding and lack of knowledge are often accountable for blindfolded positive consent of a user [2,6].

Privacy-unaware behaviour has the potential to result into passive expenses for the user. In [7], McDonald and Cranor presented a theoretical approach to determine the cost of sacrificing user privacy. According to them, user-time should be valued because service providers are harvesting profits from privacy-sensitive data. They assigned cost against required time for reading privacy policies. The total cost is calculated from the wage rate during leisure. More than $780 billion dollar was calculated as the required cost. Their result signifies the need for transparency to preserve proper privacy.

Jung et al. [4] conducted a survey on different mobile OSs users and concluded that an ‘expectation gap’ is present toward transparency and actual usage of their agreed permissions. Furthermore, Acquisti and Grossklags [1] pointed out that users are more likely to sacrifice their privacy due to misperceived consequence and lack of sufficient information. Their findings exposed the failure of the current methods in order to make informed privacy decisions.

Au et al. [3] developed PScout to analyse Android permissions and found out that 22% of the non-system entries are unnecessary. They went through several versions of Android (from version 2.2 to 4.0) and reported redundancies after examining 75 permissions. Their findings indicate the fact that personal information is being collected without informed consent of the user. Additionally, Rosen et al. [2] pointed out how difficult it can be to understand the privacy implications from an Android interface. They introduced a profile based solution to offer a better understanding by exposing behavioural statistics on privacy issues.

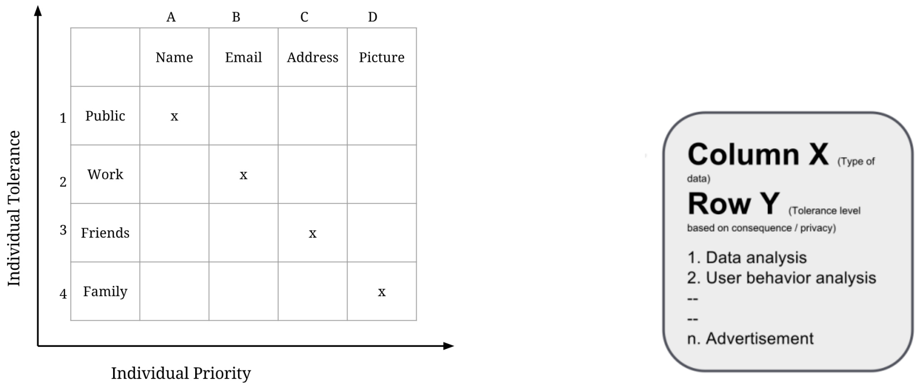
In summary, it has been confusing situation for the users when they need to decide upon their privacy. Decisions are being made with misleading perception about consequences, which lead them to leak delicate personal information involuntarily. An alternative solution is required to simplify the representation of personal data usage that should have the ability to ease the decision making dilemma by offering a clear and conclusive notification with consequences. However, the problem is two folded. First, the permission usage is provided to the user assuming that she possesses proper knowledge to understand it, which is in fact overlooked by majority. It encourages the user to ignore it and carry on without paying attention. Second, even if we are able to educate the users in an easy to understand way, tolerance threshold varies from person to person and is unquantifiable.

4 Solution Architecture

By taking into account how individually defined privacy is, and how blurry the methods are that we can use to ensure respecting it, we believe that the place to start is by improving transparency. To address the aforementioned problems, we propose a theoretical solution which is based on a two dimensional matrix structure. Initially, this method was introduced in our master thesis work.

Let us consider matrix M *(m*n)*, where m = number of data types and n = number of threshold points for individuals. Depending on the granularity of a scenario, the values of m and n can be chosen. A matrix provides flexibility for the users in two different directions. Moreover, permitting the user to shuffle the columns provides an additional elasticity to the method.

Column: Data-types are arranged throughout the columns. Each column is accountable for signifying one particular data-type. The rightmost column hosts the most sensitive data-type and the leftmost column hosts the least significant data-type. User has the flexibility to rearrange default order of the columns. It allows to emphasise on individual preferences.



		A	B	C	D
		Name	Email	Address	Picture
1	Public	x			
2	Work		x		
3	Friends			x	
4	Family				x

(a) Matrix instance.

Column X (Type of data)

Row Y (Tolerance level based on consequence / privacy)

1. Data analysis
2. User behavior analysis

--

--

n. Advertisement

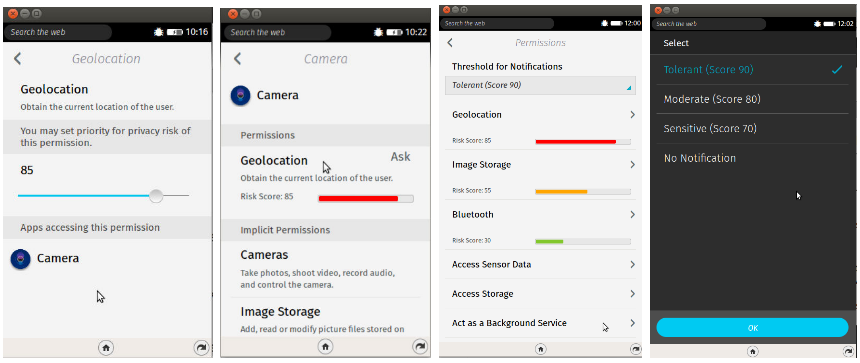
(b) Matrix element.

Figure 2: Structure and an element of the matrix solution.

Row: The rows denote a personal threshold associated with each column. As the row number increases, tolerance threshold of an individual user regarding privacy decreases. Top most row (or, row 1) denotes that the user is very reluctant about the consequences. On the other hand, the bottom row (or row N) denotes her preference about certain data to be set as the most protected one. It can also be described as follows: the intersection element of the last column and last row indicates the most strict user privacy preference for the most sensitive data-type.

Let us elaborate the scenario with an example, as illustrated in Fig. 2a, which depicts an instance of the matrix *N (4*4)*. Personal preference of user-data or, personal priority is plotted on X axis. Y axis signifies individual tolerance. For this instance, we have four different data-types which are arranged throughout the columns (A, B, C and D) according to the preference of a user whom we can call Alice. The rightmost column signifies the most sensitive data for her. It should be noted that Alice has the freedom to shuffle the columns for changing her preferences. On the other hand, selection of rows allows to modify her own tolerance level. In this case, choosing an audience for shared data is considered.

Fig. 2b shows an element of the matrix. Besides knowing about data type and default tolerance level, it can describe the expected consequences within convenient description along with appropriate references. This allows the users to go in deeper explanation if they want to. It also allows them to decide upon the clauses more precisely. Moreover, users are able to blacklist the settings if they do not want to agree. Suppose, Alice puts C3.45 as her privacy preference. This means that her tolerance level belongs to row 3 for the data type placed in column C, while denying to agree with fourth and fifth clauses. From an element of the matrix, the user is able to explore more about the types of data being shared with service provider. The user can also get a better idea about the



Geolocation

Geolocation
Obtain the current location of the user.

You may set priority for privacy risk of this permission.

85

Apps accessing this permission

Camera

Camera

Camera

Permissions

Geolocation Ask
Obtain the current location of the user.
Risk Score: 85

Implicit Permissions

Cameras
Take photos, shoot video, record audio, and control the camera.

Image Storage
Add, read or modify picture files stored on

Permissions

Threshold for Notifications
Tolerant (Score 90)

Geolocation
Risk Score: 85

Image Storage
Risk Score: 55

Bluetooth
Risk Score: 30

Access Sensor Data

Access Storage

Act as a Background Service

Select

Tolerant (Score 90) ✓

Moderate (Score 80)

Sensitive (Score 70)

No Notification

Figure 3: Interface of our prototype app on Firefox OS.

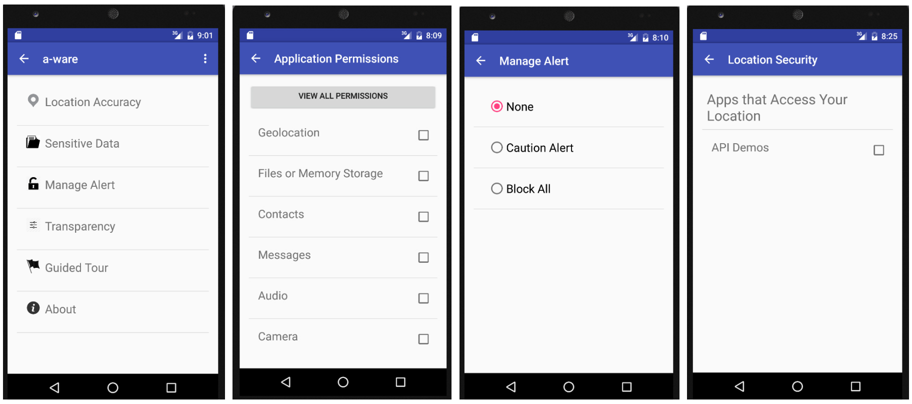
consequences of sharing such data. Finally, they can have a fine grained decision making opportunity to agree with the privacy terms and conditions.

This solution is covering only the theoretical aspects of the problem. Dimensions of the matrix depend on the depth of the proposed solution. Value of a matrix element is also subject to specific scenario which can be taken from a convenient interface. This method is partially realised during implementation.

5 Prototype Apps

We have implemented prototype apps on two different platforms: Firefox OS and Android. Having system privileges, these prototypes can show a list of installed apps along with the corresponding permissions, describe the reasons and allow users to set their privacy preferences depending on how they perceive the implications. Primarily the prototype allows the users to take a look into two lists. Installed apps are given in the first one. The list can be sorted based on privacy risks. User may carry on to discover more details about any installed app. The app details option shows the list of permissions which are being used by that particular app. In the second list, all the permissions are being populated. Users can select one and find out more to be aware of consequences. Moreover, the user may choose to receive notifications for privacy sensitive information usage by other apps.

In order to highlight the privacy-sensitive applications, we introduce *Permission Priority*. It allows a user to prioritize the apps according to perceived consequence. User-defined priority for personal information depicts empowerment over individual privacy. We also introduce smart alert mechanism for certain permission usage. The prototype offers control over notification frequency. The user is in charge to decide on when to get notification and what to be notified about. We also introduce coloured *Risk Bar* to improve awareness about consequences instantly with less effort.



9:01

a-ware

Location Accuracy

Sensitive Data

Manage Alert

Transparency

Guided Tour

About

8:09

Application Permissions

VIEW ALL PERMISSIONS

Geolocation □

Files or Memory Storage □

Contacts □

Messages □

Audio □

Camera □

8:10

Manage Alert

● None

○ Caution Alert

○ Block All

8:25

Location Security

Apps that Access Your Location

API Demos □

Figure 4: Interface of the prototype app on Android.

As shown in Fig. 3 and in Fig. 4, Alice can set her priority for a particular data-type which is equivalent to arranging the columns in the matrix solution. It allows to prioritize the apps according to potential risks. Additionally, she can get the summary of the data that is being accessed by an app. Also an overview of sensitive data usage can be visualized along with their priorities. A coloured risk bar helps her to be cautious by highlighting the risky permissions. It improves awareness of the consequences. It also rises curiosity to discover more in order to feel safe. Moreover, the prototype allows to set the frequency of notifications. The threshold is chosen by the user. This functionality signifies the choice from rows of the matrix solution structure.

5.1 Permission Priority

The purpose of placing permission priority is to introduce a user-defined scale for privacy tolerance. Considering the theoretical matrix solution described in previous section, it symbolizes shuffling the columns through setting priority. In the detail interface of each permission, depicted in Fig. 3, we introduced a *Sliding Bar* with a range from 0 to 100. It has 20 default positions within this range which means the interval between them is 5. This scale signifies individual privacy tolerance for that particular permission. Selection of highest slider value indicates maximum privacy concern of the user.

We considered two constraints to define the scale. First, a flexible enough range is required to resolve decision making dilemma. Secondly, unexpected and fine grained transparency might result into burdensome responsibility. Thus we chose high values and less number of preference taking points in order to present an optimized solution. Chosen values are used to trigger the *notification*. Finally, these values are used to be visualized as the *Privacy Risk Bar*. Persuasive power of data visualization was chosen in order to achieve good practice for privacy preserving behaviour. This risk bar offers a visual representation of safety zone and danger zone for privacy implications. User defined *Permission Priority* is also responsible here to define the colour code: green, yellow and red zone.

For the prototype on Android, we applied a different approach to take permission priority. Instead of taking values from the range of a sliding bar, check box is placed to take users' preference.

5.2 Notifications

We introduce fine-grained transparency in our implementation. Users can get alerts in order to be aware of privacy sensitive information being accessed. Moreover, the control to receive privacy alert belongs to the user. It depends on the values of *Permission Priority* and user defined threshold. The notification is triggered on extreme risks (permission priority 90 or above) by default. However, users have the option to change the threshold for the notifications in order to control the frequency:

Tolerant Threshold: Notification is triggered when the current application uses a permission having user defined priority more than or equal to 90. The user is expected to receive less amount of alerts.

Moderate Threshold: Notification is triggered when the current app uses a permission having user defined priority more than or equal to 80. The user is expected to receive moderate amount of alerts.

Sensitive Threshold: Notification is triggered when the current app uses a permission having user defined priority more than or equal to 70. The user is expected to receive frequent alerts.

No notification: Threshold for notification is set to 110. As the maximum priority can be 100, no alert will be fired.

6 Discussion

Firefox OS provides descriptive and cumbersome representation of privacy policy during the installation of an app. Users are expected to go through lengthy text. It compels a user to ignore and carry on without paying any attention. Lack of knowledge makes the situation even more difficult for users to perceive proper implications. Additionally, individual emotion and judgement can play pivotal roles behind decisions regarding privacy. This is where we identify the requirement of personalised scale for convenient individual decision making. An alternative is required to simplify the representation of privacy policy which should have the ability to ease the decision making dilemma by offering a clear and conclusive notification with consequences. In comparison with the current scenario, our prototype app is eligible to introduce solutions to the aforementioned problems.

Android offers a much better representation of permission usage on a mobile phone. Considering Android Lollipop (version — 5.1.1) and the previous two versions, a summarised permission list is provided during installation. However, users do not have any other alternative but to accept all of them. This rigid structure encourages a user to proceed without putting further thoughts on privacy implication. The latest version (6.0.1) of Android – Marshmallow – introduced runtime permission structure. In this case, user-consent is required while a user is using the app. It is indeed convenient for the user to understand the permission structure properly. Our prototype is able to complement the current scenario by adding notification for certain permission usage.

Our observations have pointed out that the present trend requires security measures to prevent invasion of personal data. However, individual privacy remains vulnerable to several attacks due to lack of proper knowledge. Often users remain uninformed about disclosing sensitive information. Misconception regarding consequences is usually responsible for privacy-unaware behaviour. Absence of easy to use tools and complex representation of permission usage play pivotal roles behind these bad practices. Sometimes subscribers are compelled to compromise their personal information in order to use certain services. It is hard to convince them to use a proactive approach while only rigid binary options are provided. As a result, users tend to ignore the privacy statement which leads to uninformed decision making towards disclosing private information unintentionally. Our two main observations are: (1) individual preference cannot be taken into a stiff framework, and (2) flexible transparency and personalized tolerance scale are required in order to design user friendly tools.

7 Concluding Remarks

Our proposed solution can provide instant overview of privacy implications. It might help users to make informed decisions. Moreover, it offers flexibility to accommodate individual preferences. It also allows the user to have personalised scale to determine their preferred boundaries. We have developed two prototype apps named AWARE for the Firefox OS and Android. In AWARE, the user can assign priorities to each permission in order to define her tolerance threshold. Our implementation depicts proof of concept for the theoretical solution. Both apps are capable of providing privacy overview of a phone. Instant notification relieves the user from worrying about disclosing privacy worthy data. As our implementation work contained privacy threat detection only, we intend to address privacy protection in our future work. Our plan also contains empirical studies to measure usability and to achieve proven viability for the prototypes.

Acknowledgment

Authors would like to thank Professor Stefan Lindskog of Karlstad University for his immensely valuable and constructive comments.

References

[1] A. Acquisti and J. Grossklags; Privacy and rationality in individual decision making; IEEE Security and Privacy archive, Volume 3 Issue 1, January 2005, Pages 26-33.

[2] S. Rosen, Z. Qian, Z. M. Mao; AppProfiler: a flexible method of exposing privacy-related behaviour in android applications to end users; CODASPY13 February, Pages 18-20.

[3] K.W. Yee Au, Y.F. Zhou, Z. Huang, D. Lie; PScout: analyzing the Android permission specification; CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security, Pages 217-228.

[4] J. Jung, S. Han, D. Wetherall; Short paper: Enhancing mobile application permissions with runtime feedback and constraints; SPSM '12 Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices, Pages 45-50.

[5] S. Patil, J. Lai; Who gets to know what when: configuring privacy permissions in an awareness application; CHI '05 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Pages 101-110.

[6] P.G. Kelley, L.F. Cranor, N. Sadeh; Privacy as part of the app decision-making process; CHI '13 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Pages: 3393-3402.

[7] A.M. McDonald and L.F. Cranor; The Cost of Reading Privacy Policies; I/S: A Journal of Law and Policy for the Information Society; Privacy Year in Review issue 2008.

[8] A. Acquisti, I. Adjerid, and L. Brandimarte; Gone in 15 Seconds: The Limits of Privacy Transparency and Control; IEEE Security and Privacy archive, Volume 11 Issue 4, July 2013, Pages 72-74.