Analyzing user awareness and deployable security solutions to prevent user data abuse through Android Permissions

Avanthikaa Ravichandran aravich7@ncsu.edu
Swathi Dinakaran sdinaka@ncsu.edu
Manogna Nalluri mnallur@ncsu.edu

Project description:

The aim of the project is to evaluate the awareness among mobile users regarding the potential privacy issues associated with permissions granted while installing applications, and further suggest scalable security usables which can detect application's non-compliance with privacy policies.

Mobile applications exceeding the granted level of permissions have previously caused security breach of information.To protect users from such information leaks, a few approaches and solutions have already been proposed.

Our main goal of the project is to analyze these proposed solutions to understand how efficiently they have worked to mitigate security risks and filter applications requesting unauthorized permissions for the users, and evaluate user's control over installing Android applications with insecure data permissions implemented.

Background and Motivation:

The purpose of requesting permissions from users for mobile applications was to improve the user's privacy and transparency. Android's permission system is designed based on the security principle of least privilege, where the permissions need to be declared. It has been observed that a few app permissions may not be necessary for app functioning; rather, an app may request access to particular permission on the device, only because a third party wants to gain access to such data which may be used for advertising and personal data processing. This poses a great risk of potential data leak.

Recently confronted privacy issues due to app permissions include Pokemon Go app, which requested permission to grant full access to the user's Google account and contact information in Android version despite being a non-multiplayer app; Meitu, Anime Makeover app, while it might seem normal to request camera access for photo editing, this app has requested permissions to access the device location, information about cell carriers, Sim card and Wifi connection information which are not necessary for the functioning of the application.

The above mentioned issues can be resolved by assisting the user in making informed decision about granting permissions to such mobile applications. Few existing solutions to resolve these issues include Appcensus, PrivacyProxy, Lumen app, Privacy assistant and Sparrow project . These approaches involve Android applications which analyse the apps and permissions requested by them and recommend apps and in some cases evaluate the security measure of application. The approaches used in existing solutions will be analysed to find the most suitable model which can best provide security protection.

Related Work:

There have been various studies that identify situations where these app permissions are misused by developers to snoop on private data. Ayed[1] published a paper in 2015 which details about the ambiguity of user permissions. He noted that, while the development environment on Android requires the user to set explicit permissions, most users do not know what the application developers do with the collected data. This gives room for the developers to carry out malicious transactions with users' sensitive data.

In the paper published in 2017, Pelet[2] discusses about the three main categories of permissions that an application can set - normal permissions, dangerous permissions, and signature or system permissions. Normal permissions do not affect the user because it only grants access to simple settings such as wallpaper management, ringtone management etc. and are given by default. The second category of dangerous permissions requires user's consent during installation. The third category, Pelet explains, is the most dangerous because it gives the application access to crucial and confidential data from mobile phones. He further expands on the lack of awareness among users about these and the dangers they pose.

To create awareness about the permissions and data that are used by free, publicly available applications, AppCensus AppSearch[3] was developed by the security group at Berkeley. This app uses a dynamic analysis technique where each app is tested in the laboratory to identify the working of the application and the actual data that is retrieved when the application runs. This allows users to look at what data is being shared and choose to control permissions on data they do not wish to share. An Android application called Sparrow[4] has also been developed to show users the permissions that are set and lists all the dangerous permissions set by each application in the device.

While these applications help users identify the permissions that are set, neither of them allows these permissions to be changed. This needs to be done manually by modifying the permissions for each app. To make this easier, an app called Privacy Assistant[5] has been developed by researchers at Carnegie Melon University which uses machine learning to not only display the permissions that are set but also suggest changes to these permissions to minimize the amount of data that is shared.

Proposed Approach:

This project is aimed at evaluating the various privacy protection solutions that identify what user data is shared and the permissions set by users during installation. It also tries to propose the best solution to overcome data leak issues that arise from developers taking advantage of naive users.

The first step in this project will be to conduct a survey among users to understand the level of user awareness. This survey will include questions which will help identify whether users know what permissions they are setting, why it is required for the application, how the collected data is being used etc. This will help us assess which areas require attention when proposing/evaluating a solution.

With this in mind, we will additionally collect data about the requirements and concerns of the users. These questions will focus on what privacy means to the user, what data he/she is comfortable sharing, how he/she would like to control the data that is obtained by the applications etc. It will also include questions related to existing solutions and whether users are

aware of them. Using this data, we can better understand user needs and can propose solutions that cater to them.

Further, we will perform a detailed analysis to evaluate existing solutions (like Sparrow[4] and Privacy Assistant[5]) based on this collected data. We have data that indicates the level of user awareness, privacy needs of the user etc. With this we will evaluate, for each solution, how easy it is to use and understand, does it have provisions or suggestions to improve data privacy, and the limitations of each approach.

Finally, we will identify either a single existing solution or a hybrid solution obtained by contrasting the various options and propose it to users for improving their data privacy on any Android phone.

Initial evaluation:

The survey containing user responses could be used to evaluate the user awareness. The criteria for evaluation include measuring the extent of knowledge the user has regarding the permissions given while installing an application. which can be deciphered by having the user answer comprehension questions regarding application permissions and the flow of personal data.This acts as criteria to measure the widespread perception regarding app permissions and its role in data leak.

Further the data collected during the survey regarding common problems faced by user due to android permissions and recent privacy issues in the news could be used to determine the issues that form a problem set. The existing solutions can be compared with the issues to determine which problems are already addressed and the ones that need to be addressed.

The response of users to different privacy preserving solutions could be analysed to understand the extent of usability of the applications and comprehension by the users.With this data, different solutions are evaluated and compared with each other to check for areas of improvement regarding usability and the best solution or a hybrid approach could be deduced.

Milestones:

Steps	Time frame
Conducting survey to understand user awareness	3 weeks
Analyzing the existing solutions	2 weeks
Suggest a hybrid solution	3 weeks

References:

[1] Ayed, A.B. (2015) A Literature Review on Android Permission System. International Journal of Advanced Research in Computer Engineering & Technology, 4, 1520-1523.

[2] Pelet, J.-E. (2016) Mobile Platforms, Design, and Apps for Social Commerce. Advances in E-Business Research Series, IGI Global, New York.
[3] AppCensus AppSearch: https://search.appcensus.io/about#aboutBrowse
[4] Sparrow - Protect your Privacy: https://play.google.com/store/apps/details?id=sa.es.sparrow
[5] Privacy Assistant: https://play.google.com/store/apps/details?id=edu.cmu.mcom.ppa&hl=en

Proposed approach:

With extensive use of mobile applications, the users have grown to ignore the obvious problems with granting android permissions. The developers and third parties exploit the user's low awareness and try to obtain sensitive information about the user. Though many solutions address the problem, there are very few that reach the targeted audience .The project aims at evaluating the awareness of user regarding android permissions, in the process identify a problem set, that the user is most concerned about regarding privacy permissions. We expand the problem set by including the privacy violations that had occurred in the recent past, which users need to be protected against, regardless of the awareness of user. The available solutions are weighed against the identified problem-set. The most viable solutions are tested for usability by the targeted audience. The best features among these solutions are identified and a product that is a combination of these features is proposed.