ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Enhanced Privacy Protection Model for Android

Amit Radharaman Pandey[1], Ahmed Ali Mujeebullah Khan[2], Sangeeta Oswal[3], Ramesh Solanki[4]
PG Student[1, 2], Assistant Professor[3, 4]
Department of MCA
VES Institute of Technology, Mumbai, Maharashtra, India

Abstract:
In today's digital era, every individual has a smartphone, laptops, computers that helps individuals to connect to internet and use various services. The most commonly and widely used way to access these services is smartphone. Often these services gather data from users to provide various services such as recommendations, advertisement etc. But the main concern over these services is that end user is unaware of how data is stored, whether data is secured or services sells these data to third parties etc. The aim of this paper is to provide an idea on how a user should use these services in order to protect and only share data that is required for services.

I. INTRODUCTION:

Nowadays almost everyone in the world have internet-enabled devices. A great part of them has been using international computer's net known as Internet. Internet has lot of advantages some of them are as follows:

1. Internet provides access to a lot of information. Some of them are very useful in your job other helps in your hobby. On internet, you can find everything you want. You can also do shopping using Internet by using different services such as Amazon, Flipkart etc. You need only to select what you want, fill in some forms In a few days you will get what you have ordered directly to your home, without going anywhere. You can pay with your credit card, pay postman when you get the package, or transfer money from your bank account. Nowadays almost every bigger bank offers transferring money with Internet. It is faster than going to the bank and filling blankets. Transferring money in traditional way takes about a day, using Internet you can do this in few seconds even on weekends. What's more internet banks give you insurance against unauthorized transaction. Some people thinks that their money can be easily stolen by hackers. It isn't true because the easiest way to steal your money from internet bank is breaking to your house and stealing you card of codes. Internet banks have very good protections witch make them practically unbreakable.

2. Internet provides email. E-mails delivers very quickly. It is very important when you want to send some information over internet. E-mails can be used to send texts, films, photos, songs, computer programs etc. Costs are very important advantage of emails. Sending an email is much cheaper than calling, or sending normal letters.

3. Internet is also coming handy for the users in connecting with their friends and colleagues. There are various social networking sites available on the internet where you can stay in touch with your friends and colleagues. Moreover, some developers have also come up with some social networks that are especially dedicated to the students and teachers. You can also recommend these social networking sites in your institution to have better communication. Above all services requires some data from users for performing different operation such as Amazon requires user's data for showing suggestions regarding product. And usually most of these services collect data from users with/without consent of users. The problem arises when data is collected without user consent and services neither shares any information to user how it uses those data collected from user.

Benefits of Data Collection:

There are various services which collects, stores and analyzes data for benefits of users as well as these data helps services to show relevant information to users. Some services which collects user data and operate on that for users benefit are Google, Amazon, YouTube, Flipkart etc.

For example:

When a user uses various services from google then google collects various kinds of data from users such as :

- Websites the user visits
- Videos that user watches
- Advertisement on which user clicks on or tap
- User location
- Device information
- IP address and cookies

and other information such as name, data of birthday, gender etc.

All these data which is gathered mostly by these kind of services are used for various user benefits such as google uses these data for:

Improving google maps services to help people reach faster to their destination Helps in auto completion of search term while using google search engine Helps in finding videos on YouTube as well as recommending in which user most probably have interest. Above example shows how a collecting of user data is essential activity to provide smooth and context aware information to user. But there are many services which abuses this activity and collects data for their benefits rather than giving priority to user. And these services neither share any information regarding how they use data.

Shortcoming of Data Collection:

1. Anyone Here Order a Taxi for Data Misuse?

Taxi-hailing service Uber consciously developed a tool it calls “God View” which, when used legitimately, allows tracking of all Uber customers in real time. However, Forbesreported that Uber often used this function as entertainment in parties showing the Ubers in a city and the silhouettes of waiting Uber users who had flagged cars. While a strong sales gimmick, one party attendee reported that real-time information was used and as a result individuals were identifiable.

2. While You Watch a Samsung TV, It Watches You

The recent Samsung TV incident clearly demonstrates this: The electronics giant admitted that some smart TVs were logging users’ activity and voice commands, but argued that a clause buried in the privacy policy stated that spoken words could be “captured and transmitted to a third-party.” The subsequent media storm led Samsung to advise customers to switch the option off on their TVs.

As the examples exhibit, data misuse is widespread and can occur in what you might think is a safe place to have your data warehoused such as large banks, telecommunications companies, and state police departments. One might wonder why there aren’t tools or processes to prevent or detect data misuse.

The truth of the matter is that many tools exist, except tools to ensure appropriate data usage have not kept up with the massive amounts of data we are now seeing. Sure, access controls prevent unauthorized users from getting their hands on personal data, but doesn’t provide visibility into how the data is being used. Compliance can validate whether a company has taken the right course of action mandated by government laws, but it doesn’t follow through to know if these actions are working or not.

Problem:

In current digital era, it is found that 80% to 85% of internet usage is contributed by mobile/smartphone users. So more often, the services are consumed by mobile/ smartphone device users. And service providers have started to provide applications for ease of use to users. These applications can gather various kind of data from user to provide different services(as described above data gathering is essentials part of service) to user such as location, user contacts, storage, call logs etc. But at the same time, these applications can also retrieve data which may not be required by application but application retrieves those data for their own benefits such as selling those data to third-parties, for advertisement etc. To put in perspective, we have gone through various application and found that there plenty of application that retrieve unnecessary/irrelevant information or data from users without user’s consent. It is also found that some application often connects to some random servers and shares anonymous data to those servers. Which should be taken seriously as these activities are taking place without the user's consent.

For example:

Many applications which are published under 'Cheetah Mobile’ account often send data to some anonymous server and also request for some unnecessary permission such as internet which is not required for functioning of application at all. Another example could be some wallpaper application which we encountered during our research asked for some permission which are eventually not required by application at all. A simple and concrete example could be an application known as 'True Caller'.

The main functionality of this application is similar to DNS i.e. this application helps to resolve/get name from phone number. But the question here is how do they do that? Do they contact mobile phone operator for such information?

To answer the second question, it is very clear they don't get those data from mobile phone operator. So now the only question remains are how they resolve phone number to name and how do they get data? So they provide these service of phone number to name is by collecting data from users of application.

True caller application collects user’s contacts and store it in their database without consent of user. And how they use these data apart from providing above service is unclear. So it is recommended to have a strict modal to prevent such kind of data collection by application.

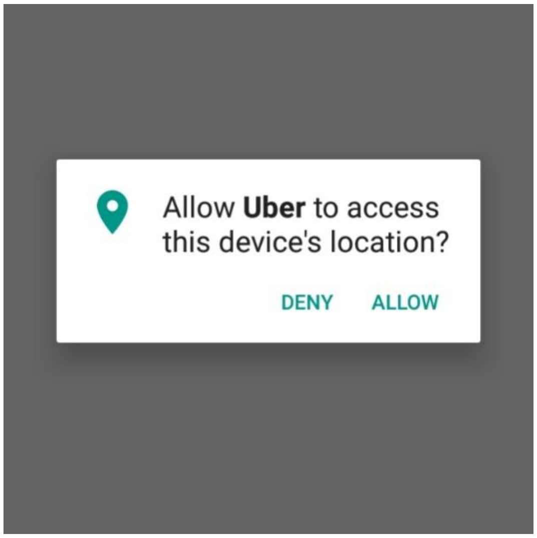
All though to tackle these problems, there are some solutions that are already proposed such as Granular Permission Control (Ask for permission when required). But in our research we found that these modal is not enough to give the complete control of data in user’s hand.

For example, in current modal, no application is required to ask for internet permission. Which we think as major drawback in current modal. As every application is having access to internet, they can easily abuse these pre-defined permissions and send data to some servers although that application doesn’t require an access to internet for any of its functionality.

Solution:

Fine Grain Permission Control:

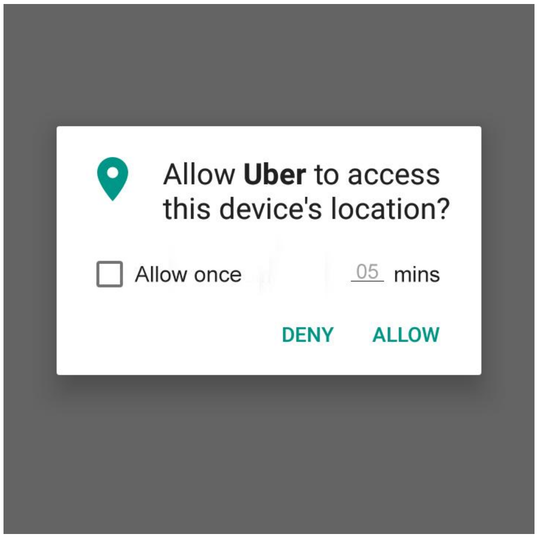
A solution for this problem could be is provide complete controls to user over data and what features/functions of mobile device an application is allowed to use should be placed under control of users.



Allow **Uber** to access this device's location?

DENY ALLOW

Current

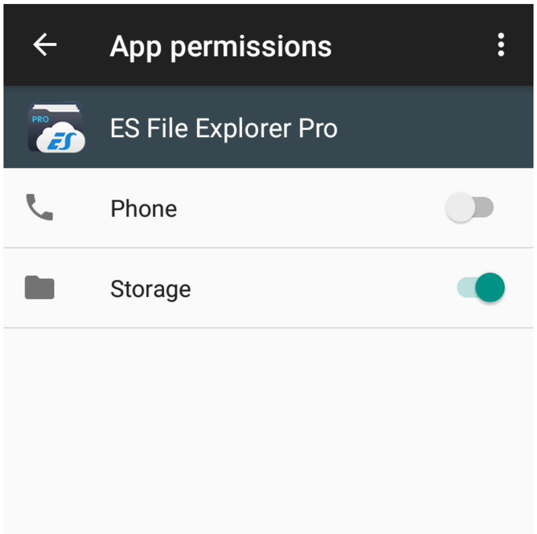


Allow **Uber** to access this device's location?

□ Allow once 05 mins

DENY ALLOW

Proposed



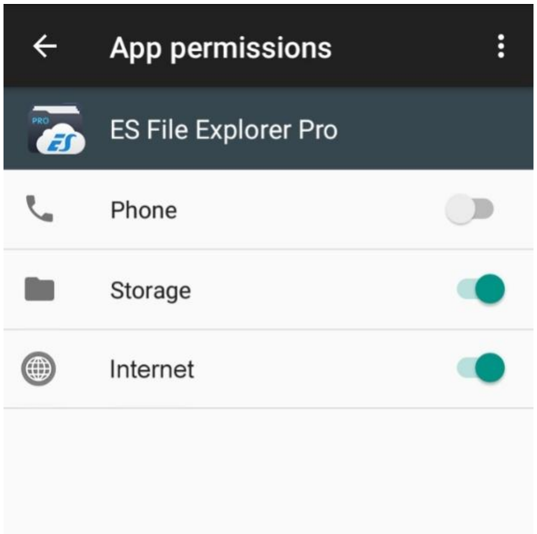
App permissions

ES File Explorer Pro

Phone

Storage

Current



App permissions

ES File Explorer Pro

Phone

Storage

Internet

Proposed

For example:

Every application should request for every permission which is required and no permission should be assumed/preset to application (internet in current modal). Another addition to this modal could be to allow to particular permission for one-time usage which is missing in current modal. Such as allow particular application to use internet for next half an hour so. So this technique of restricting application after some period time can greatly help to prevent sharing of user's data without their consent. And this above purposed modal should apply on all permission which sends some data across network to provide functionality such as location sharing, contact access to application etc.

II. CONCLUSION:

Data of users is very precious. Data can be used for various purposes (for benefit of users as well as against users). So we should build a concrete modal to protect those data from unintended as well as unauthorized access to data. And the above purposed modal could very well protect that data of user from unintentional sharing of data.

III. REFERENCES:

[1]. https://privacy.google.com/your-data.html

[2] http://www.targetmarketingmag.com/article/when-data-collection-goes-wrong-10-examples- identity-data-being-misu se d/

[3]. https://developer.android.com/training/permissions/ reques ting. html

[4].https://blog.hootsuite.com/social-media-security-for-business/

[5].https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/9-social-media-threats-you-need-to-be-aware-of

[6]. https://www.sophos.com/en-us/security-news-trends/ security - trends/social-networking-security-threats/ facebook. aspx