A Study of attractive android apps and its threatening security issues

Prof. Mahesh Sawant
Sinhgad Institute Of Computer Sciences, Pandharpur, India
mahesh.sawant07@gmail.com

Prof. Rakhi Sonawane
Sinhgad Institute Of Computer Sciences, Pandharpur, India
rakhi.rakhisonawane@gmail.com

Prof. Aarti Kalani
Sinhgad Institute Of Computer Sciences, Pandharpur, India
aartikalani07@gmail.com

***Abstract*— Use of mobile applications in the current era is improved nowadays in a vast amount. The advancements of the Smartphone generation are responsible for cyber attacks. This paper focuses on android applications which are free of cost in google play store and android market and its security issues, this paper also focuses on how the users are getting attracted towards free apps of android.**

***Keywords*— Android Apps, Smartphone, Security.**

INTRODUCTION

The era of cellular communication has changed its way smarter by the use of smart phones. Before 2010 the cellular communication was only the concern of cell phone usage for people in India. Later on people moved their way to become smarter by using smart phones and its uncountable features. 95% of the cell phones today are smart phones and having android as an operating system.

Android is well known operating system which is mostly used in smart phones. Android Market and Google Play store has almost around 7,00,000 plus applications (a.k.a "Apps") to keep its users entertained. Android is famous just because of its numerous apps available in the market. Music, movies, games, reminders, maps, news, emails, social applications, messengers, etc are the types of apps available on android markets. Out of the 7 lakh apps, around 6 lakh apps are free of cost. Some renowned app developers charge some amount of money for their apps to be downloaded and used. The large amounts of apps are making android more and more popular. Android is an operating system which is user friendly and interactive. So people are getting attracted towards it, as it is open source. Open source concept of android is allowing its uncountable developers to download the code of OS freely and use it as per their needs. Many of the device making organizations are using android source code and developing their own apps and selling the handsets, tablets and smart phones. On the other hand the attackers and spammers have raised their hands on the users of android market. The free apps developed by attackers may lead to fetch the data of users SIM card, Phone Memory, messages, etc. Now a days the smart phone users are using the internet connection with them all the time during the day. Also its impossible for people to carry their Credit cards, debit cards, cheque books, etc with them, so people used to save their account details in Messages, account numbers in Contacts, etc. This is the reason the spammers and cyber attackers are getting the full access to the data of android users. This issue haven't. been covered by Google yet, so this paper focuses on all the above discussed topics. This is one of the most harmful topic of the current users.

HISTORY OF ANDROID

Android is one the mobile Operating System, which was initially developed by Android Inc, in 2003, later on in 2005 Google backed it financially and bought it in the same year. The smart phone user's number changed rapidly in 2008 when android sold their first mobile phone with the new Operating system named Android. The uniformity of android was more comfortable for people, so people welcomed android with a huge response. Later on Android had no option in the market. It was only the cell phone which was sold 94% of the mobile phones in 2012.

EASE OF USE

Android is the most efficient and popular mobile platform where people can have access to around 7,00,000 applications in Google play store, a location where the uniformity of the android is achieved, each and every application used on android OS is kept in the cart name Play store, so that people can have the access to apps just with the single click. example, the most famous app now a days is **whatsapp** which is a messenger service based on internet costing free to people. Can be accessed through play store of the Google only.

STEPS TO DOWNLOAD APPS FROM PLAY STORE

1. Search for Apps:

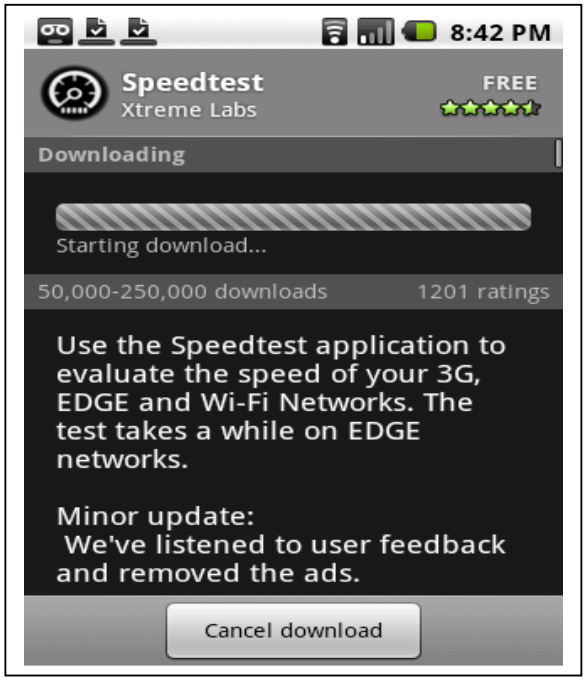
One touch connectivity to play store is inbuilt in the android OS, if the user wants to search for some app, he has to visit to the play store where the apps are available free and some are paid. You can search for the app name, or app type it will give you the entire related search. The search box in the app store allows you to type anything related to your desire app. It searches from the app store and gives you everything related to your searched app.

The following image depicts us the search criteria of the play store in android.

The above image shows us how to search on play store.

2. Installing an App:

The 7,00,000 entertaining, music, videos, games, etc apps on android allows users to download and install the application on their smart phone. Installing an app firstly requires to download the app from android play store. The following image guides us how it downloads from the store.

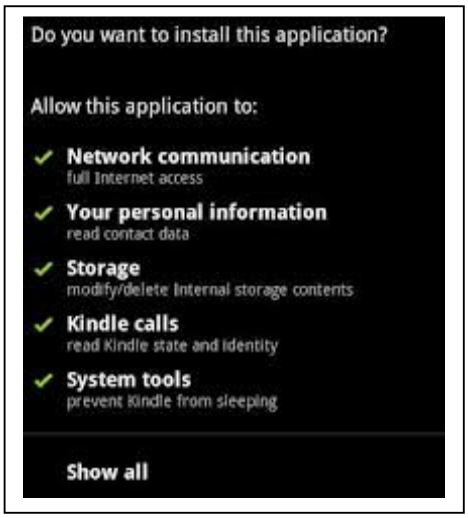


As soon as the app is downloaded from store, it is now ready to get installed automatically. After completion of its download, it automatically starts installation. This is one of the background process of installation and there your app is installed in the menu list.

3. Authentication:

While installing an app to the android smart phone, app developers are taking the advantage of users installation, during installation the app asks the user to have access to the various things such as Memory card (storage), Contacts, SMS, Phone Memory, Call log, etc. Here Some apps are providing check boxes so that user will select which component is to be shared with the app. But some of the apps are not providing the check boxes they are directly tell the user that we need the access to such things,

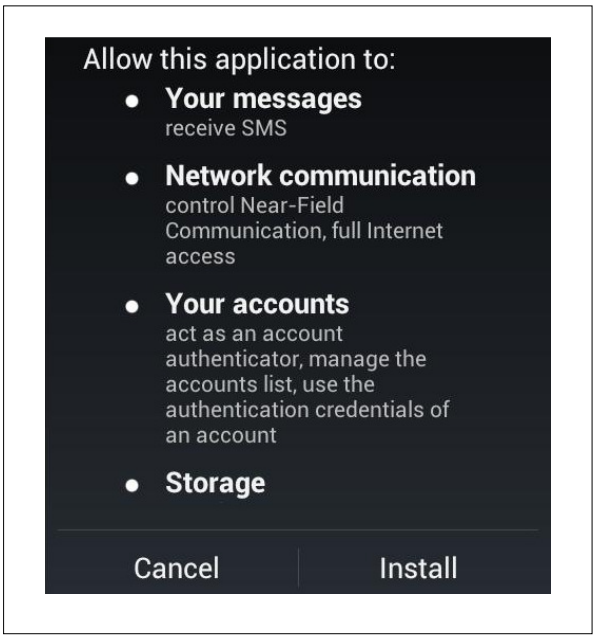
The following image shows the concept of authentication,



This above image shows us that how it wants have an access to the components of cell phone. And also have a look at the following image which shows us that, it do not ask for any check boxes, this gives the developers a direct chance to access all the things those are mentioned here, In a survey, it has seen that, users are too eager to download and use the app, so they are unaware about what the app is asking for. In the picture below, the mentality of the users is sticking to one thing that each and every app needs the same thing. So each and every time the android user don't pay much attention only because the uniformity of each and every app. Some of the organizations may not use the mentioned data, but how we can be more reliable that every app maker don't use the mentioned information.

By providing the access to phone memory, memory card, contact book, SMS, etc. whenever the app user is connected to internet connection, the data stored in the phone memory it could be personal images, videos, data sheets, any personal information will be directly accessible to the app developer and he can have access to the personal information of all the users data. This may lead to the data loss or crime in cyber usage. The app maker can be a cyber attacker or a spammer too. This app maker can use the users' data for many purposes.

As discussed above, it has has seen that cell phone users are getting smarter by using the smart phone, he is using the internet on the palms or in pocket all the hours of the day. Also smart phone user is not using other gadgets (pockets, wallets, etc.) that's the reason the smart phone users are storing the personal information, bank details, etc on the smart phones in various ways, either in contacts, in the SMS, or he can save a word, excel file of his passwords too in the memory card. If such information is lost and accessed by hackers he may hack the data, money from various passwords of online banking, credit cards and debit cards, etc.



Look at the image above due to which above mentioned things are possible for the hackers, spammers, or cyber attackers.

The data may be lost every time when the user is connected to internet. During this time user is unaware about his data loss. The application may ask for the updates, and user may get attracted towards its update. During update process also the data can be lost in a large amount and rapidly. To prevent such type of data loss of the users, we suggest android some solutions through the patch of software to check the security of an application.

SOLUTIONS

The android applications are more entertaining, so that users are downloading and using the app in a large number. The above mentioned problems are found very frequently. The large amount of data is shared on the internet just because of these apps. We are providing two solutions to android for such a security check and stop the data loss. The two solutions through this paper are as follows:

Solution 1:

We are working on some application software or patch development in which we are concentrating on the app developers originality and actual presence. This process of authenticating the developer includes collection of its personal details such as name, address, contact numbers (both landline and mobile numbers) organization name, email address, etc. with these details only the user will be authenticated and checked actually for the details he have provided during the authentication. By getting authentication he will be able to upload an app on play store and android markets. Even if the single detail is not provided by the developer he will not get authenticated and he would not be able to upload the app on the store. Also the developer will get a verification code each time during upload of a new app, he will have to put the same code which our system will send him the SMS on his registered cell phone. This process of authenticating the developer will help the regular and normal developer to get develop the apps and be popular in the market. It will also avoid the spammers, cyber attackers and criminals to get away from android, as the personal information asked by android will be verified, so the illegal tasks will be avoid.

Solution 2:

Even if some app require the access to the phone memory, memory card, SMS, phone books, contacts, call logs, it should be in the hands of user who is downloading the app. Many spammers are making this process so complicated, There is no need to have an access to such things. Even if it is not required or required, it should be decided by the user solely that to which component the app can have access. The installation process should make the use of check boxes for such an information. This will help the user of app to get more reliable on the app and its developer too.

Finally, the two solutions through this paper will help and android developer and user to be more reliable. The software patch will work as a Barry gate to spammers and cyber criminals.

I. CONCLUSION

By using the more flexible application authentication process user can be more and more reliable on the application developer. This will help users to be relaxed about their data. There will be no spammers and cyber criminals in the community of the android app developers. This is most important for the users of app and Android too.

REFERENCES

Android Applications Security, Paul POCATILU Bucharest University of Economic Studies, *Informatica Economica,* vol. 15, no.3/2011

www.spicesteller.com

http://android-ssl.org/Why_Eve_and_Mallory_Love_Android__An_Analysis_of_Android_SSL_(In)Security/android-ssl.org.html

An Analysis of Open Security Issues of Android Interfaces to Cloud Computing Platforms by Corey Andrew Beres.

Mobile threats: Android most vulnerable Times of India, by: Ankit Upadhyay.

Angela Moscaritolo.2011,*"Significant security threats found in Android devices" http://www.scmagazineus.com.*

Threat Analysis of Android Market, T.venon., D.Stroop.,GTC Research,2010, http://globalthreatcenter.com

http://www.h-online.com/security/news/item/Encryption-found-insufficient-in-many-Android-apps-1732847.html

ANDROID PROTECTION SYSTEM: A SIGNED CODE APPLICATIONS THESIS Jonathan D. Stueckle, Capt, USAF, AFIT/GCE/ENG/11-06 SECURITY MECHANISM FOR SMARTPHONES.

[11] Security Issues in Smartphones and their effects on the Telecom Networks - SAGHAR KHADEM, Chalmers University of Technology, University of Gothenburg, Sweden

[12] BRIDGING THE GAP BETWEEN PRIVACY AND DESIGN**,** *Deirdre K. Mulligan**, *Jennifer King***

Address Space Randomization For Mobile Device, H.Bojinov. Dan Boneh., Rich Cannings.