ISSN No. 0976-5697

Volume 3, No. 5, Sept-Oct 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.inf

Possibilities Of Android Phone Based Cyber Crimes Due To Security Permissions – A Critical Study

Mr. Parag H. Rughani*
Assistant Professor & Head
Department of Computer Science
Christ College – Rajkot, Guj, IN
parag.rughani@gmail.com

Dr. H N Pandya
Professor & Head
Department of Electronics
Saurashtra Univerisy – Rajkot, Guj, IN
hnpandya@yahoo.com

Abstract: With the official launch of Android, Google has reached to the hands of mobile users. As per the survey android occupies around half of the mobile market share. This clearly indicates dominance of android phones. As android phone has many advanced features, it has many vulnerabilities and issues that can compromise end-users' privacy. This paper concentrates on those vulnerabilities and privacy related issues. The paper includes discussion about android permissions and possible threats including cyber crimes. We have also explained how it can permissions can be easily mis used in applications for hacking user's data and resources. The practical implementation explains the experiment in detail. Certain possible solutions are also listed which can help in improving safety of android phone users.

Keywords: Android, Cyber Security, Privacy, Confidentiality, Cyber Crime, Permissions, IPhone, Java ME, Android Market, Android Applications, Data Theft, Threat, Risk, Personal Information, Resources, Security

I. INTRODUCTION

Google android has attracted people from around the world by its features and user-friendliness. As per the latest survey done by comScore's in February, 2012 [1], almost 50% of US smart phone mobile market is dominated by android phones.

Top Smartphone Platforms
3 Month Avg. Ending Dec. 2011 vs. 3 Month Avg. Ending Sep. 2011
Total U.S. Smartphone Subscribers Ages 13+
Source: comScore MobiLens

	Share (%) of Smartphone Subscribers		
	Sep-11	Dec-11	Point Change
Total Smartphone Subscribers	*100.0%*	*100.0%*	*N/A*
Google	44.8%	47.3%	2.5
Apple	27.4%	29.6%	2.2
RIM	18.9%	16.0%	-2.9
Microsoft	5.6%	4.7%	-0.9
Symbian	1.8%	1.4%	-0.4

Figure 1. Share of different vendors in US Smart phone Market

Being an open source android is attracting mobile device manufacturer companies to develop new designs and specifications with android as an operating system. This allows companies to provide devices with cheaper rate and more features compare to other competitors. Samsung is one of such companies and has covered a good market compare to Nokia and Apple by having Android with it.

From user's point of view Android is more suitable because it is more user-friendly and has many additional features. Even though companies like Apple and RIM give similar features in their Iphone/ Ipad and Blackberry devices respectively, they are costlier compare to Android devices. This is one of the major reason in India where people are purchasing android devices more.

Android is more famous because of its applications which are available on Android Market (Now Google Play). There are millions of applications under different categories, which attracts users as per their interests.

As every technology has advantages and disadvantages, android is also not an exception.

In this paper we have tried to find out some of the vulnerabilities in android OS which may lead to loss of personal data and information.

The research work involved in this paper is based on Android 2.2 Froyo and equivalent versions.

In the next sections we will explain how android permissions work and can be mis used by hackers in compromising end user's privacy.

We have developed a working application which fetches user's data without his/her knowledge and sends them to web server if Internet connectivity is available or if it is not then it sends same information through SMS.

At the end few suggestions which can be useful in maintaining privacy up to certain level..

II. ABOUT ANDROID

A. *Android is open Source [2]:*

One of the biggest reasons behind popularity of Android is that it is Open Source. Here it is very important to understand that when any product is declared as open source its complete source is published openly.

The advantages of open source technology are many but there are few disadvantages. Especially when you open complete source code of any operating system, people can easily understand the internal mechanism and if the code has any vulnerabilities then it can become very easy to get into system unethically.

The open source aspect of Android allows third-party developers to develop applications and developers can easily access low level libraries and resources for their application use. It is always good for developers' fraternity but never for end users. Not all developers are good neither all applications

are worth to install. The madness of using free applications can lead to sever loss of data. This is one of the biggest disadvantage of using Open Source Technologies.

III. ARCHITECTURE OF ANDROID OS

Since Android is based on Linux Kernel, architecture is very similar to any Linux flavor. Following figure depicts the very similar Android OS architecture.

In following figure the first and second layers from the top are more of our interest. Even though these layers are indirectly dependent on remaining layers, they are the layers which can be used by developers to get access of the resources.

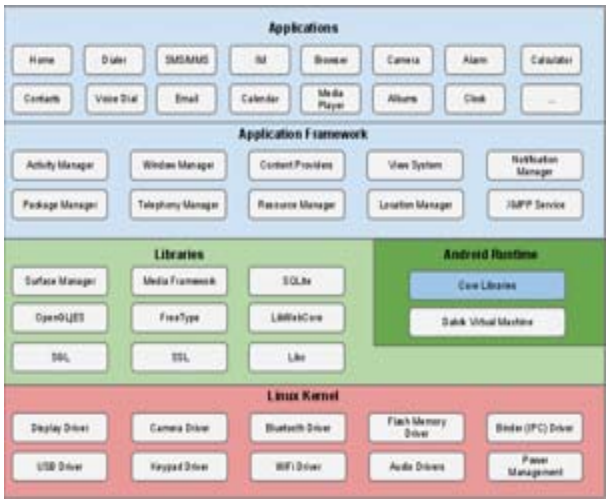

Figure 2. Android OS Architecture [2]

The Applications and Application Framework layers are very critical from the securities point of view. Application Framework is available for developers so that they can develop applications for android platform.

For a third party application, access to Linux kernel or library can be achieved through Application Framework and which is being available to the developers.

It does not mean that any one can access application framework without user's knowledge. Android has a feature called permissions, which needs to be granted by the end user if any application wants to access any resources on that particular device.

IV. PERMISSIONS – THE SECURITY MEASURE IN ANDROID

In this sub section we will compare implementation of permissions in Android and other mobile technologies like Java ME and IPhone.

Many people do not like Java ME based applications as they annoy users by prompting them for permissions whenever there is a request from running application. Even though it is bit disturbing as it asks every now and then, application settings from the device can be used to allow/deny access of any resources permanently.

But, the best part about this approach is whatever resource has been demanded by the application is not accessed without user's permission. In short things executed by your Java ME application is always known to the end user [3].

For example if a Java ME application tries to access contact details or send the SMS, proper prompt will be shown to user for getting permission. If user feels that its fine, let the application do it he can allow and if it is required very frequently then he can change the setting to allow the access permanently.

This is implemented because Java ME is a programming language and applications developed using it can run on any devices/operating systems having support for Java. So, here different operating systems may have different security policies and it is always better to inform user about such critical transactions through programming itself.

It becomes very annoying if it asks for permissions during the execution. For example you have installed an application to synchronize your contacts and text messages on the web server, it will ask you for accessing contacts, inbox and network connection. So if you say yes to a prompt asking for access to contacts, another will come to ask for another permission, and you may feel it disturbing.

This is one reason why this implementation frustrates Java ME Application users and may be the reason why new technologies like Android are adopting different approaches.

The same concept of permission has been adopted by Android but in different way. Android applications also warn user about access required by application but only at the time of installation. The funny thing is there is not any button called accept, rather it shows the required permissions and two buttons called I***nstall*** and ***Cancel.*** So if you click on install it means you are granting the permissions asked by the application. And if you feel that certain permissions are doubtful, you can press cancel [which will quit the installation] [2][7]

Following figure is a snap shot of one of the application setup screen which asks the user about required permissions in Android phone.

Figure 3. Permissions Requested by an Android Application during installation.

The reason behind asking for permissions at runtime is user-friendliness. So it tries avoid those annoying prompts during the execution. Another advantage of such logic is to make sure that user understand the permissions needed by the application in advance and only install it if he/she has no objection on giving permissions. In other words its kind of license or agreement we see during the installation of any application, so if you don't accept it will not continue with the installation.

As you can see from the above figure that all the permissions are not displayed together in the screen. Due to small screen size in mobile devices/smart phones, only first few permissions can be seen there. If you want to see all the required permissions then you will need to scroll till bottom, which common users don't do in general.

At the time of installation if user does not refer to the permissions mentioned then it may happen that he may grant some unwanted permissions which can cost him loss of data or information.

Following list gives an idea about few important permissions which can be used by developers for getting access to your resources.

Table I. Android Permissions and Their Meanings [4][9]

Permission	Meaning
BLUETOOTH_ADMIN	Allows applications to discover and pair bluetooth devices.
CALL_PHONE	Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call being placed.
READ_CALENDAR	Allows an application to read the user's calendar data.
READ_CONTACTS	Allows an application to read the user's contacts data.
READ_LOGS	Allows an application to read the low-level system log files.
READ_SMS	Allows an application to read SMS messages.
SEND_SMS	Allows an application to send SMS messages.
ACCESS_FINE_LOCATION	Allows an application to access fine (e.g., GPS) location
WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage

These are only few of the important permissions provided by android. These permissions can be set in AndrodManifest.XML file during the development.

There are few other permissions which can allow the application to change wifi or phone state, install application, observe activities on the phone, use camera, etc...

All these permissions give the freedom to develop any type of applications and access mentioned resources.

V. ANDROID MARKET

In this sub section we will discuss how applications can be installed on android and compare the process with IPhone. The section also contains details about Android Market.

If we see how IPhone applications can be installed then we would be able to compare same process of android with better understanding.

In IPhone the applications should be installed only from Apple Market [for internal use, it is not compulsory to publish the application in market]. And during the development phase for testing purpose a provisional certificate provided by Apple is must for installing the application. This provisional certificate contains UDIDs [Unique Device ID] of the devices, and only those devices can install the application. Once the application is developed and tested thoroughly can be published in the Apple Market[5].

Now during this publishing process Apple verifies the code of the application, and many other things before it gets published. If any error is found the application will be refused.

I like the way this complete process is handled by Apple, because they are keen about users and are not giving freedom to third party application providers for entering into users' devices.

Another constraint in IPhone applications is selection of the application to be published in IPhone market. If application to be published is found to be not very useful or is similar to other existing applications then in many cases such applications are rejected by Apple.

Now if we consider installation process in Android then its very liberal and flexible [6].

First of all any application can be installed to any device directly by just checking ***Unknown Sources*** in Settings → Applications. Every android application contains an in-built certificate which can be used for installation. This allows developers to test the application.

Second major drawback of Android Market [Now, Google Play] is it allows any third party application to be published without any checks or restrictions and that is the main reason why Android Market has millions of applications. Many of those applications are useless and have common features.

Again, if we compare Android market with IPhone then the code of the application is not checked before publishing, so it may contain buggy or faulty applications.

Due to above flexibilities and freedom developers can publish and/or install any application on the Android Market. [8]

Majority of cyber criminals publish their applications in the form of games, adult applications or entertainment and fun related applications in ***Free Applications Section***, because majority of applications are downloaded from this section and malicious code can be easily distributed through it.

VI. PRIVACY & CONFIDENTIALITY

If we consider that an application using critical permissions is installed on user's device then it can play with your privacy and confidential information. Specially the permission which access Internet connectivity and SMS can easily send important information from your device to the criminals without your knowledge.

Following are few examples which illustrate how applications can fetch my data.

Example 1: If an application on my device can read my text messages, calendar activities and contact numbers then there are chances that my personal communications and data can be sent to the hacker. These data later can be used to know about my daily activities and my near ones. Which can affect my social and personal life.

Example 2: If an application on my device can read my current location then any one can trace me at any time without my knowledge and again it compromises my privacy.

Example 3: If an application can read my notes, memos or files then it can compromise my confidential information to the hackers or criminals. These data can be related to my credit cards, user accounts, business plans or job opportunities.

Example 4: If an application can access my Gallery then it becomes very easy for criminals to get photographs or videos from my phone. These photographs or videos can be very personal or private and if it goes outside my phone without my knowledge then it can be very harmful for my personal life.

These are a few examples of several conditions where important data can be taken out of an android phone if user does not know about it.

VII. POSSIBLE CYBER CRIMES

Based on above discussion, now we can think about possibilities of Cyber Crimes through Android devices. If your device is infected with an application which internally uses your data or resources without your knowledge then it is possible that you can be victimized by cyber crimes, here we cannot ignore possibilities of traditional crimes [with android device as a too] also.

Following are few conditions where such malicious applications can get installed in your device and use your resources or information without your knowledge:

a. You do not know anything about permissions and you install the application.
b. You do not know about all permissions and you grant permissions without looking at them [as all the permissions cannot be seen together in small screen]
c. You have accepted permissions during the installation but you do not know which permission can use which resource or data from your Android phone.
d. You know that installed application is accessing your data or resource for your usage, but you do not know if it is being used unethically.

So, by any means if your android phone is infected with any such vulnerable application then you can either yourself become a victim or you can become a media for any crime.

If criminals can get your personal information, your daily activities, your locations, information about your relatives or friends, etc... then they can keep watch on you and your close ones and plan out crimes accordingly.[10]

Few possible crimes can include: Money Laundering, Identification Hacking, Account Hacking, Kidnapping, Murder, Rape, Robbery, Fraud, Abuse, etc... [criminals can fetch the information from the android devices and can commit traditional or cyber crimes.]

Here we cannot ignore possibility of Terror Attack, as terrorists are using latest technologies more and can misuse this weak feature of Android.

VIII. PRACTICAL IMPLEMENTATION

When we came to know about severity of android permissions we developed a testing module to confirm whether things happen in that way or not.

We developed an application for Android 2.2 with following design and features.

A. Objective:

Developing an application that can fetch end user's personal information from the device without his/her knowledge.

B. Definition:

The application can be used to retrieve information of Actors and Actresses from Film Industries. The application never asks for any information from the user. So, user will always feel that he is only getting data from the web server, he will never feel that his data is going outside his phone without his knowledge.

The information comes from web server and application has to be connected to Internet for using it.

C. Concept:

Whenever user will make a request to web server, two simultaneous threads will run. One will fulfill user's requirement and will be in front, while the other one will run in background and without user's knowledge it will fetch user's information from the phone and will send them to web server.

So when user requests any information, he will see a progress bar or activity indicator saying "Loading... Please Wait", user will not doubt on the application as he has requested data from the web server and loading image may take some time. The background thread in the application will run simultaneously with the front thread and user can never know what is happening in the background.

D. Design:

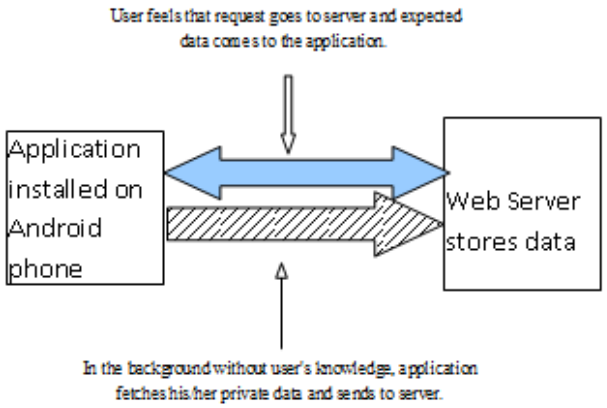

Figure 4. Design of the Test Application

E. Features:

a. User can browse images and information of Actors/Actresses of Film Industries from web server through Internet.

Reason: looking at common people these type of applications are downloaded by more users compare to other applications and utilities.

***Permission*:** Internet Access [wifi, 3G, etc...]

b. User can save photographs to their Gallery *Reason:* Users would like to save photographs to their local device for setting them as wallpaper or may be for off-line use.

Permission: Access to Gallery

c. User can save my contact number and can send me message or call me or my customer care for giving their feedbacks or suggestions.

Reason: People trust on the applications having contact details and if then can contact customer care or application provider.

Permissions: Address Book, Phone Call and Inbox.

d. User can see if any Actors/Actresses are available near to their current location.

Reason: People would like to know which of their favorite actors/actresses are near to them at any time then they can see them personally.

Permission: User's Current Location

Here even if user will study the permissions then also he/she will feel that all these permissions are needed and mandatory for the application, so will grant those permissions and will install the application without any hesitations.

e. Testing:

We tested application on different emulators and real devices including Samsung Galaxy Ace, Samsung Galaxy Y, Samsung Galaxy S, Android Developer Phone, etc...

In first version we found that fetching and uploading approximately 300 contacts and 100 messages from user's device takes around 45 seconds. So, we divided process of fetching user's information in different executions and it can be done in unnoticed time.

f. Conclusion of the experiment:

This experiment was carried out to confirm vulnerabilities found in Android platform, specially by the permissions. If hackers can convince users for the permissions then they can easily misuse those permissions to get private or confidential information stored in user's device.

Thus we need a powerful and more secure android for protecting possible cyber crimes, which can be committed based on user's private and confidential information.

IX. PROPOSED SOLUTION

I have worked on Android Source Code (AOSP) and modified some of the files to create a log file which can keep track of URLs accessed by applications installed in the device.

Android source uses file called DefaultClientConnectionOperator.java in the folder /external/apache-http /src/org/apache/http/impl/conn/ to maintain client connection operator.

The function openConnection() in this file is responsible for opening a connection to the URL, requested by the running app.

The function takes five arguments, out of which first argument is of HttpHost and it contains the URL for which connection needs to be opened.

In my solution, I have used this function for keeping track of URLs called by different applications.

These URLs can be stored in a simple text file or in other format as a log file, which in turn can help the user to see which URLs are accessed internally and by which applications.

This helps in analyzing and identifying unwanted applications running on the device and connecting to suspicious web servers.

In the next step, I am working on searching the data which is being transferred on that URL. This will keep track of URL and data being sent or received to that URL.

X. REFERENCES

[1] http://www.comscore.com/Press_Events/Press_Releases/2012/2/comScore_Reports_December_2011_U.S._Mobile_Subscriber_Market_Share (ComScore Press, February, 2012: Available at)

[2] http://developer.android.com/guide/index.html

(Android Developer)

[3] http://developers.sun.com/mobility/midp/articles/permissions/

(Java Me Security Permissions)

[4] http://developer.android.com/reference/android/Manifest.permission.html

(Android Manifest Permissions)

[5] http://www.apple.com/itunes/

Apple itunes [The Application Sore]

[6] http://market.android.com. (Android Market)

[7] W. Enck, P. Gilbert, B. gon Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth., "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones". In Proceedings of the 9th Usenix Symposium on Operating Systems Design and Implementation, August 2010, pages 393–408,.

[8] Michael Grace, Yajin Zhou, Zhi Wang, Xuxian Jiang . "Systematic Detection of Capability Leaks in Stock Android Smartphones" - Proceedings of the 19th Network and Distributed System Security Symposium (NDSS 2012), San Diego, CA, February 2012 (17.8%).

[9] Alastair R. Beresford, Andrew Rice, Nicholas Skehin , and Ripduman Sohan., "Droid: Trading Privacy for Application Functionality on Smartphone." In proceedings of Twelfth Workshop on Mobile Computing Systems & Applications, HotMobile '11, May 2011.

[10] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri., "A Study of Android Application Security." In Proceedings of the 20th USENIX Security Symposium", USENIX Security '11, August 2011.