Analysis of Security Trends and Control Methods in Android Platform

Payal Mittal
M.Tech (CS&E)
Amity University
Noida,
payalmittal6792@gmail.com

Bhawna Dhruv
M.Tech (CS&E)
Amity University
Noida
bdhruv08gmail.com

Praveen Kumar
Assistant Professor
Amity University
Noida
pkumar3@amity.edu

Seema Rawat
Assistant Professor
Amity University
Noida
srawat1@amity.edu

***Abstract*- We all are familiar with smart phones and their technical & functional enhancement which makes user life much easier. There are thousands of applications present in play store today which fulfils our everyday life's needs. These Online Application Stores gives user hundreds of thousands of application in one minute. All users are aware of the fact that any individual run its application in play store with no such high restrictions and policies. It is due to android environment in which applications are only verified through mechanism of digital signatures along with coarse grained grant from server developers of android ecosystems. Recently IccTA surveyed a range of approximate 3000 real-time based applications with accuracy of 88% and founded around 150 interlinked security leaks in 20 applications. These days, a high rate of privacy data leaks comes under surveillance which arises due to feeding personal information into heterogeneous applications. It is a big challenge for the debuggers to trace security procedures and policies to prevent data leakage. In this paper, we describe methods of detecting and preventing android privacy leakage through privacy control mechanisms of android systems.**

***Keywords*- Smart phones; Android Applications; Malicious Activities**

I.INTRODUCTION

In the Past, Android was a less known term for users in smart phones. But today Android completely changes the definition of mobile phones. It brings all the developers together to a common platform for variety of opportunities being provided. Android is developed by Google as developers have to pay very less code certification fees to be android their working platform [1]. As android is developed from past few years, number of applications also increased in the same pattern. Individually it is possible that any place you go, downloading and installing any application from Android Market and App Store becomes so easy and free to use which gives just one click method for thousands of mobile users. As a result, to use these applications user must have to give its personal information details like access to his photos, location details, e-mail ID, contact number etc. which further misuse by application developer, then it become a security concern [6]. The security policies and procedures of smart phones and heterogeneous devices become a critical issue for mobile owners. For users, it is very important to aware of the mobile operating system in which mobile system works. The most widely known systems are Android, Symbian, iOS, RIM and Microsoft, in which Android and iOS are most commonly used by end users. The major flaws of Android platform are as follow:

- Absence of central repository server to control privacy which means there is no security mechanism present when information is communicated between device and server.
- Almost all applications ask to feed the personal information into location based social networks so it failed to hide data from unauthorized user.
- It is very difficult to find the present location of user because as most applications are based on GPS but these applications store data in database and unable to extract it efficiently.

There is no centric database present that results in many severe data problems like backup, portability problem etc.

Let us consider an example when an army man in combat zone is working with his smart phone to click photos of enemy regions. After his complete vigilance, he connects his device with Wi-Fi and sends his entire confidential data picture to high authority of Surveillance Company. In between the sending process of authorized images, an illegal user hacks the network channel and gets confidential data abruptly. This illegal user is hired by enemies of army known as terrorists. Through these images, they will able to vacate the regions promptly and hence security breaches are exploited. In this particular case, there is an urgent need to implement device image attacks prevention techniques like authentication of images before sending them to network, locate double data bases for login credentials etc. [11]

II. LITERATURE REVIEW

Researchers have discovered many weaknesses on Android devices as it is a open source system developed by Google. Android has Google Play Store which is a hub of different applications and any individual user is able to put their application into play store by using Software Development Kit. Google claimed that they designed a framework of security for Android platform which includes essential policies like a grant system of different access method with respect to every new application demands and sandboxing technique which is basically a method of placing virtually enabled interface or walls between each application and software on the machine [2]. In addition, android's latest version 4 have biometric security identified as BehavioWeb which periodically checks mobile user Keystroke and platform usage pattern. The fast application development of Android is achieved from its Open Alliance Version. An Android consists of a numerous number of applications which are written in Java language. Developers have to use Android API to build all applications in this platform. Individual application is inserted into a jar file (.apk). This operating system uses a form of UNIX sandboxing for continuation of running applications. All applications have privileges; they can communicate with each other through IPC mechanism. In this mechanism, all the security and configuration parameters are defined in one file called Android Manifest-Xml.

A. Android Architecture

As we already mentioned, Android Operating System is based on Linux and comprises different core set of libraries. The architecture model of Android System is shown in figure 1 that has Linux server at the lower level, then Android middleware and finally heterogeneous applications are embedded into this model.

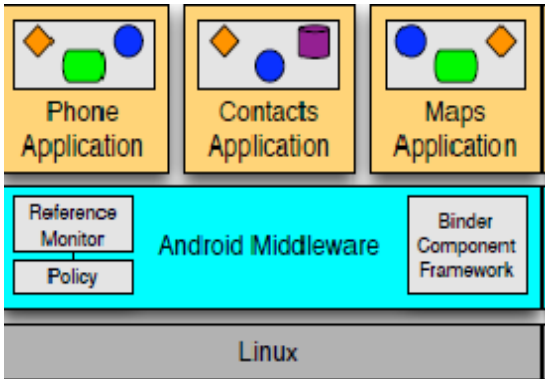

Fig. 1 Architecture Model of Android [7]

B. Android Application Model

An android application contains different application parameters and components as seen in fig. 2 i.e. Content Providers, Activities Planning, Services and Broadcast Domain Receivers. The

Fig. 2 Components of Android Application [16]

Manifest file in IPC mechanism must declare all the components in application and application requirement also. There is a different role of each component in isolated application characteristic and developer has to activate each application individually[3].There is certain working methodology of components of Android Application which can be best understood with the help of figure 3.

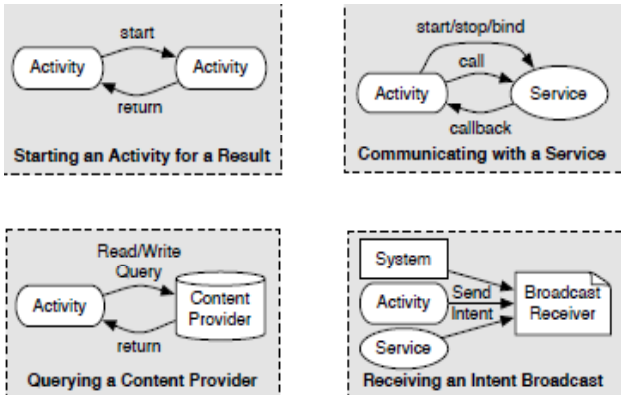

Fig. 3 Working Methodology of Components [5]

C. Multiple Layers of Android Security

According to Google, Android has multiple layers of defense to protect its platform from malware attacks but this can be or have exploited by unauthorized user. Attackers have the special technology solutions to break the security of Android applications. Fig. 4 shows the multiple layers of Android Security Mechanism.

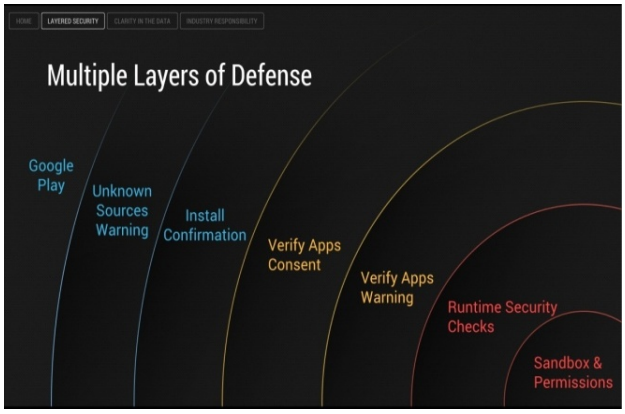

Fig. 4 Multiple Layers of Defense [13]

As a user, we can only have Google Play through which we can download any application but actually when an application is downloaded it has gone through six security checks i.e. Sandbox and Permission, Runtime Security Checks, Verify Apps Warnings, Verify Apps Consent, Install Confirmation, Unknown Sources Warning and then finally permission is granted from Google Play [9].

III. CRUCIAL ANDROID SECURITY

This section proposed a brief introduction of critical private setting issues that have been faced by the users on Android applications. Each application demands personal information and user do not have knowledge of how personal data is exploited for misusage by unauthorized user. As we know, Sandbox is a basic method used in Android mobile phones. The methodology of Sandbox works in two ways- First by using application's manifest file Android Manifest.Xml for permissions and second by mapping different user ID with application. This concept improves the privacy of applications in Android operating systems.

A. Privacy Issues in Android Applications

Following are some privacy issues in Android applications which are discussed below [4].

- Smart phone Identifier International Mobile Equipment Identity Number (IMEI) is track and identify for misuse. Unauthorized User change mobile phone IMEIs to alter blacklisted IMEIs with valid IMEIs.

- SMS misuse will enable mobile users to loss of rights and assets. Mainly, the payment related credential SMSs in smart phones, makes mobiles the center point for attack.

- Attackers use user's physical location for misuse which is one of the most confidential information. It becomes very easy for thieves to steal the devices through tracking on mobile phones by location based search engines.

- It is almost impossible to find out and prevent the adware attack in smart phones as browser history contains heterogeneous sources of downloads.

- Mobile Users cannot install all versions of operating systems which have enhanced functionalities and they are also required to pay the extra charges for sharing of mobile internet connection with any desktop.

B. Privacy Prevention Model of GPS in Android

During the application installation through software development kit, Android scrutinize the AndroidManifest.XML once only at the beginning stage, after that Android has no permission grant mechanism to inspect application.

```
01 // get GPS Manager Instance
02 GPS Manager Location Manager = (Location Manager)
03this.get SystemService (Context. GPS_SERVICE);
04 // Define a location listener to receive GPS updates
05 GPS Listener LocationListener = define Listener ();
06
07 // add the GPS listener to the Location Manager
```

```
08GPSManager.requestUpdates
(LocationManager.NET
09 WORK_PROVIDER, 0, 0, location Listener);
```
Current Privacy Control Method in Android [17]

It is only job of application to ask for permission for using GPS services as shown in figure 6. To recognize the security control methods implementation in Android, we develop the following code to understand the working of security control ways of Android [17].

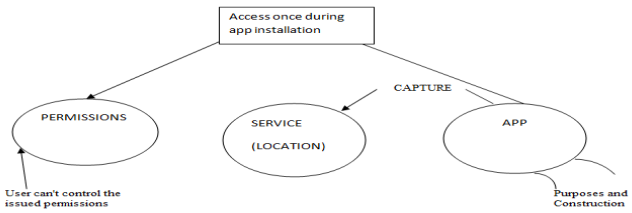

Fig.5 Android Privacy Control Model of Android [21]

C. Assessment of reinforcement of Android Security Platform

The assessment on Android operating system makes it highly reliable for malicious attacks by illegal users. There exists certain loop holes into Android Software Development Kit and emulator which makes it vulnerable to threats and risks of attack [19].

Development tools Accessibility	Yes
Platform Amiability	Yes
Setting Up Vectors	Multiple
Application Flexibility	Yes
Application Testing	Yes
Application Discernment	Yes
Unauthorized Repositories	Yes
API Signing & Limits	Yes
Distribution Estimation	No

Table1. Development of Android Assessment [12]

Numerous loopholes are described below in Android System [15]:

- Extensive use of eminent platform language-JAVA.
- Adequate serviceability of Android API.
- At the instant of writing code, application becomes portable between versions of Android.

IV. RECOMMENDATIONS

A. For Android

It is well known for Android platform that any application can be feed into Android Market with too less restrictions and security policies. Android allows self-signed applications that nowhere check the content of code present at back end of that application. It depends on user's download rate and comments on application for malware protection. There is only one method to remove application from market i.e. when enough people register complaints for a common application. This type of scenarios proved beneficial for attackers to manipulate. App store has better privacy and security than Android platform. A method called source code checking provides a stronger protection to Android Market against vulnerability attack by replacing it with reviewer comments and crowd sourcing.

B. For Users

From the start, try to build security and privacy planning to hide the data of smart phones. Assure data that is no longer needed, delete it and if any is stored, store in encrypt form [8]. Do not transfer data off the device without encryption technique. Instead of raw data, hash values should be used. User should be careful with third party code. For precaution, user should clean their browsing history records form mobile phones. Users also need to have some anti-virus software which has ability to protect against malware [10]. An efficient method for Android Market is Intrusion Detection and Prevention System (IDPS) to protect the privacy of smart phones.

CONCLUSION AND FUTURE WORK

In General terms for mobile users, there persists no solution to hide and protect personal access data in Android smart phones. In this paper, we highlight the Android platform security problems and how easily can unauthorized user steal all the data of thousands in one instant. It is also clear from the paper that Android Security concepts not only need software platform applications but also the hardware assumptions. In addition to security and privacy problems, there exist chances of malware attack also. We also review some attack prospective and recommendations for both Android platform and mobile users for possible precautionary measures. In the future, we will elaborate highly effective privacy

approaches through which we can prevent malware attack from thieves and also the concept of phone-based sandbox technique to protect encryption of data.

REFERENCES

[1] William Enck, Machigar Ongtang, and Patrick McDaniel, "Understanding Android Security", IEEE Security and Privacy Magazine, January 2009.

[2] Aubrey-Derrick Schmidt, "Detection of Smart Phones Malware", In: Dissertation, Technische Universitat Berlin, Germany 2011.

[3] William Enck, Damien Octeau, Patrick McDaniel, and Swarat Chaudhuri,"A Study of Android Application Security", Proceedings of 20th USENIX Security Symposium, August 2011.

[4] H.Kuzuno, "A Proposal of an Information Flow Checking System for Android Application", Computer Security Symposium 2011 (CSS2011), ID2-2, PP. 155-160, 2011.

[5] T. Blasing, L. Batyuk, A-D Schmidt, S.A. Camtepe, and S. Albayrak, "An Android Application Sandbox system for Suspicious Software Detection", Proceedings of the 5th International Conference on Malicious and Unwanted Software, 2010.

[6] Android Open Source Project, Android Security Overview, http://source.android.com/tech/security, October 2012.

[7] R. Fedler, J.Schutte, and M. Kulicke, "On the Effectiveness of Malware Protection on Android", Fraunhofer AISEC, April 2013.

[8] H.Lockheimer, "Android and Security" February 2012.http://googlemobile.blogspot.com/2012/02/android-and-security.html.

[9] Asaf Shabtai, Yuval Fledal, Uri Kanonov, Yuval Elovici, Shlomi Dolev, and Chanan Glozer, "Google Android: A Comprehensive Security Assessment" IEEE Security and Privacy, 8:35-44, 2010.

[10] A.Apvrille, "Cryptography for Mobile Malware Obfuscation" RSA Conference Europe, October 2011.

[11] Leonid Batyuk, Mackus Herpich,Sey it Ahmed Camtepe, Karsten Raddatz, Aubrey Derricck, Sahin Arbayrak,"Using Static Analysis for Automatic Assessment and Mitigation of Unwanted and Malicious Activities within Android Application within Android Application", 6th International Conference on Malicious and Unwanted Software, 2011.

[12] Alexios Mylonas, Sechos Dritsas, Bill Troumas, Dimitris Gritzales," Smartphone Security Evaluation: The Malware Attack Case", Department of Informatics, AUEB.

[13] Rafael Fedler, Marcel Kullicke, Julian Schutte," An Antivirus API for Andorid Malware Recognition", 8th International Conference on Malicious and Unwanted Software, 2013

[14] Roland Schmitz, "Mobile Malware Evolution and the Android Security Model".

[15] Giovanni Rusello,Bruno Crispo, Earlene Fernandes, Yuri Zhauniarovich,"YASSE : Yet Another Android Security Extension", IEEE International Conference on Privacy, Security, Risk and Trust,2011.

[16] Emre Erturk," A Case Study in Open Source Software Security and Privacy: Android Adware" World Congress on Internet Security, 2012.

[17] Mohd Alhamed, Khalid Amier, Mansoor Omair, Nei lee," Comparing Privacy Control Methods for Smartphone Platform", IEEE, MOBB, 2013.

[18] Christoph Stach, "How to Assure Privacy on Android Phones and Devices", 14th International Conference on Mobile Data Management, 2013.

[19] Dong Surfars, Mongjum Xie, "Secure Intelligence Gathering Using Smartphones", IEEE, 2012.

[20] Li Li, Alexandre Bartel," I Know What Leaked in Your Pocket: Uncovering Privacy Leaks on Android Applications with Static Taint Analysis", April, 2014.

[21]LocationStrategies,"http://developer.android.com/guide/topics/location/strategies.html.