The International Journal Of Engineering And Science (IJES)
||Volume||2 ||Issue|| 3 ||Pages|| 56-59 ||2013||
ISSN: 2319 – 1813 ISBN: 2319 – 1805

Implementing Security on Android Application

[1,] Kirandeep, [2,] Anu Garg
[1,] *School Of engineering and Science, Lovely Professional University*
[2,] *G.T. Road, Near Chehru Railway Bridge, Phagwara (Punjab)-144401, India*

----------Abstract----------
In these days, Android has become a very popular operating system for smart phones. There are some advanced features in android Smartphone, with which user can easily share applications via online market store i.e. Google market store. But, there are attacks and threats include in this platform, like malware applications are also attack on Android actual applications. Because malware on device can create number of risks, which creates problem while connectivity because of security issues. In this paper, it will be described that how security can be improve of Android Operating System so that users can safely used the android smart phones.

Keywords: *Android, Security, Encryption, TISSA.*

Date of Submission: 2 March, 2013 Date Of Publication: 25 March 2013

I. Introduction:

An Android is an open source operating system, key mobile applications having API libraries for executing android applications. Android smart phones offers advanced computing ability and connectivity as compares to other mobile phones operating systems. Android is operating system which designed hardware so that communication between hardware and software with user interface can easily be done. Google has released tool i.e. Google apps that implement under some security policies. There are so many facilities like password protection also implement in android smart phones. Android is Linux based operating system. The architecture of android operating system is designed in such manner so that communication at application level and end user will be quite easy. Android applications are written in Java, a programming language. But Android has its own virtual machine i.e. DVM (Dalvik Virtual Machine), which is used for executing the android applications. Android applications also run on non-mobile household devices like oven, AC, refrigerators, washing machines etc. Designing of android application is easy as compared to other applications of iphones. Android operating system is also used for business purposes. At business level, risk will be high while transferring data from one end to another end. As Android provides remote access to official sensitive data, which can lead to data hack if smart phones are hacked into. For this security purpose, Google has designed their operating system to execute applications in specialized sandboxes, which minimize the capability of malware attacks to the applications in smart phones.

1.1 ANDROID ENCRYPTION:

Disk encryption on Android operating system is based on dm-crypt, which is kernel feature that works at block device layer. It works with flash devices which present themselves to the kernel as a block device. The file system to use on these devices is ext4. It is an independent either encryption is used or not. Linux kernel is doing the encryption work. The actual encryption used for file system for first released was 128 AES with CBC. The master key is encrypted with 128 AES to the openssl library. By adding new module to void and its components, it will invoke encryption features. There are commands like checkpw, restart, changepw and crypt complete used for encryption on android operating system.

1.2 How to enable encryption on a device?

Android is designed having multi layer security which provides flexibility for this platform. When attackers attempt attack on device, android platform help to reduce the portability of the attack.

There are key components of android security which are described as follows:

a) **Design review:** when a security model is designed then it will be reviewed by the developers so that risk level will be very less while using the model. When risks come, immediately teams for controlling risk factors will start work on that to reduce the risks level.

b) **Code review and penetrating testing:** the goal of this code review is that in which it will be checked that how the system will become strong?

c) **Open source and community review:** android uses open source technologies that have significant external review such as Linux kernel.

d) **Incident response:** android team enables the rapid mitigation of vulnerabilities to ensure that potential risks to all android users are minimized.

II. Review Literature:

In android operating system, there are four layers, which are described further in detail. Android has its own libraries; it is helpful for developing and designing any application of android platform. These libraries are written in C/C++. Linux kernel is the 1st layer which is written in C. Linux also helps to wrap the application in android.

The architecture of Android operating system is described in detailed as follows:

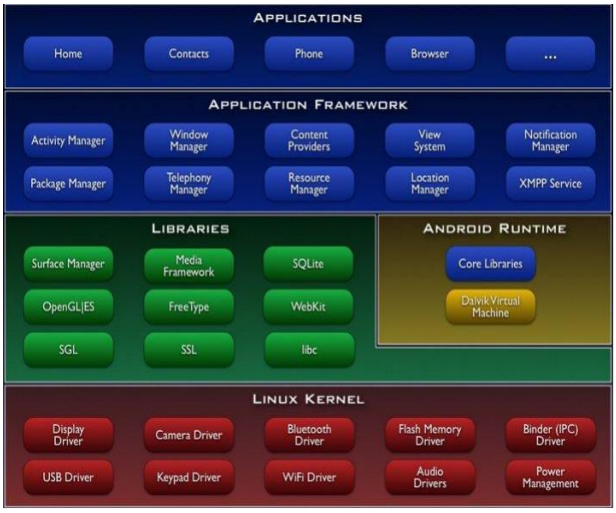

Fig 2: Architecture of Android Operating System [1]

Application layer: It is the most upper layer in android architecture. All the applications like camera, Google maps, browser, sms, calendars, contacts are native applications. These applications works with end user with the help of application framework to operate.

Application framework: Android applications which are developing, this layer contain needed classes and services. Developers can reuse and extend the components already present in API. In this layer, there are managers which enable the application for accessing data. These are as follows:[5]

Activity manager: It manages the lifecycle of applications. It enables proper management of all the activities. All the activities are controlled by activity manager.

Resource manager: It provides access to non-code resources such as graphics etc.

Notification manager: It enables all applications to display custom alerts in status bar.

Location manager: It fires alerts when user enters or leaves a specified geographical location.

Package manager: It is use to retrieve the data about installed packages on device.

Window manager: It is use to create views and layouts.

Telephony manager: It is use to handle settings of network connection and all information about services on device.

Android runtime: In this section, all the android applications are executed. Android has its own virtual machine i.e. DVM (Dalvik Virtual Machine), which is used to execute the android application. With this DVK, users are able to execute multiple applications ate same time.

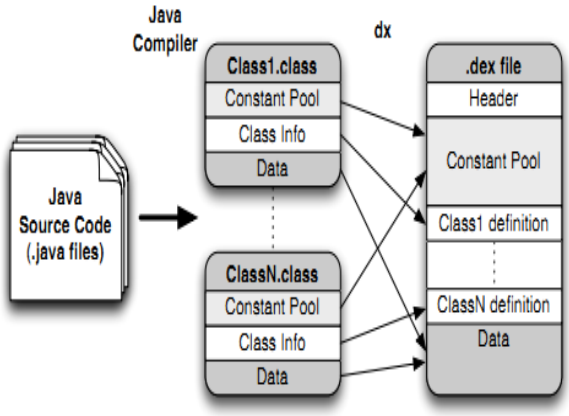

Fig 2.1: Dalvik Virtual Machine Process[2]

Libraries: Android has its own libraries, which is written in C/C++. These libraries cannot be accessed directly. With the help of application framework, we can access these libraries. There are many libraries like web libraries to access web browsers, libraries for android and video formats etc.

Linux kernel: This layer is core of android architecture. It provides service like power management, memory management, security etc. It helps in software or hardware binding for better communication.

Security in android app:
According to review, there is a research paper on security issues on android smart phones. Paper is Taming Information Stealing Smartphone Applications (TISSA). In this paper, TISSA is a system which is used to provide security to the contacts, call logs etc. By using TISSA, user can easily protect its contacts and call logs by filling all the permissions.

After giving all the permissions, user can easily access its own data in very privacy mode. TISSA is evaluated with many of android apps which are affected by leakage of private information of user. TISSA uses efficient CPU, memory and energy etc. In TISSA, there are main three components are used which provides security to the user for securing call logs and contacts. **These main components are: Privacy setting content provider:** It is used to provide current privacy setting for an installed application. **Privacy setting manager**: It is for the user that he/she can easily update the privacy setting for the installed application. **Privacy aware components:** These are enhanced to regulate the access to user's information which also includes contacts, call logs and locations. TISSA starts works when user sends request through installed app to the content provider. It holds the request and check current privacy settings for app. It matches all the stored information in database and then send result back to the content provider. If all the information is correct then it allows the user to access the data otherwise it will reject the request.

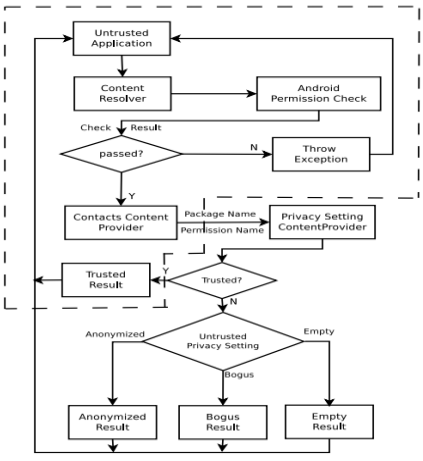

Fig. 3. Protecting Contacts in TISSA. [3]

There are main three components used which provides the security to the user, these all are as follows:

Contacts and Call Logs: In the above diagram, it shows that firstly, user sends request for accessing the app. When request sends then content provider checks all the permissions if these all are matched only then user can easily access its data otherwise it will reject the permission request from the user side.

Phone Identity: Each mobile phone has its unique IMEI number for using GSM and CDMA technologies. In android app can easily use various functions and retrieve privacy setting for requesting app.

Location: Here is location manager which always noticed about user's location. If user change its location, the registered location updates location information of the current user.

III. Conclusion:

As per discussion of this paper, it provides all over security to contacts, call logs and location or phone identity, but still there are some issues while using this system. While using TISSA, as per system use sometime it will send bogus or fake replies to the user corresponds to their request. These fake replies could create problems for some applications of android. Another issue in this system is that TISSA only uses one single privacy setting for one type of private information. To provide more security this system can be improved so that user can easily access this app in a friendly manner. Another issue is that there is no any guidance to use these privacy settings. So, this should also be improved.

IV. Future Work:

As there are some issues in this system related to security. In this dissertation, I am trying to improve security in an android app like call logs. In TISSA, only security is provided by using privacy setting, but I am doing on encryption on call logs. In these days, security is major issues while using any application. So, with the help of encryption security will increase and user can easily save his/her own private data like call logs and all the contacts. With help of encryption algorithms like AES we can easily make this application secure in better way.

Refrences:

[1] Wilner Nina (2009) " Android On Power Architecture", ELC, Grenobles.
[2] Enck William, Octeau Damien, McDaniel Patrick and Chaudhuri Swarat "A Study of Android Application Security", Department of Computer Science and Engineering, the Pennsylvainia State University.
[3] Zhou Yajin, Zhang Xinwen, Jiang Xuxian, W.French Vincent "Tamming Information Stealing Smartphone Application", Department Of Computer Science, NC University.