Forensic Analysis of Android Smartphone

Manohar Yadav
manohar.eng@gmail.com

Anand Chourasia
a.chourasia@gmail.com

Abstract: **Android is a new operating system for mobile world. Android Smartphone use the free, open-source Linux as the underlying operating system, which allows development of applications by any software developer. It is designed to run on different types of Devices. But due to its open source nature and flexible programmable framework, it leads the Android system vulnerable to get virus attacks. This paper presents the threats related to android system, their vulnerability, some controls to preserve them. The advanced computational capabilities and other advanced features have made smart phones holder of confidential user data. This study unveils the security risk associated with the use of Android Smartphone. This paper discuss the main challenges in front of smart phones and show the new research area that needs to be addressed.**

Keywords: Android, Smartphone, Forensics

I. INTRODUCTION

Android is the fastest growing mobile operating system in the recent years. The open source nature of the android makes it more attractive for the mobile companies. As it is open in nature so changes in it can be done according to the requirement. It provides a vast platform for the developers to explore the android operating system capabilities. Various developers provide applications to the user through android market, internet etc. If proper security measures are not applied by the developer then it may put the application at risk. Other than the application user's data is also at risk. Hence, vulnerable applications must be identified from the genuine one to provide the user better functionality.

As malicious applications are continue to rise in the android market, the need to investigate these applications is also necessary. To investigate these applications and their impact on the phone environment; android forensics comes into play. The focus of such investigation is to determine the suspicious and malicious applications and present the truth, which often leads to prosecution and conviction. Dramatic increases in the numbers of Android crimes; led to the development of a whole slew of Android forensic tools. These tools ensure that digital evidence is acquired and preserved properly and that accuracy of results regarding the processing of digital evidence is maintained.

In android application forensics, log files play an important role in order to find activities of the application. Log file contains log entries that provide the information regarding the application activities. If log files are properly analyzed then it can give specific information that can be useful to determine the evidences of attacks.

Applications logs also play an important role in order to find out the traces of the applications. Application database, internal files etc. can also be in forensic examination. These traces contain information that may be useful in several situations, such as attack detection, fraud and misuse of phone resources. For each type of situation, some log entries are generally more likely to contain detailed information about the activities in question. Other log entries typically contain less detailed information, and are often useful to correlate the events recorded in the log files. To understand the behavior of the application, first of all android architecture need to be explored.

II. ANDROID ARCHITECTURE

Basically android is based on Linux operating system with some further changes has been done in its kernel module. Drivers like Camera driver, Audio driver has been added to support video and audio functionality. Android is a set of middleware, Operating System and Applications. The architecture of the Android Operating System is as follows:

<table>
<tr><td colspan="2">Application layer</td></tr>
<tr><td colspan="2">Application framework layer</td></tr>
<tr><td>Library layer</td><td>Dalvik virtual machine</td></tr>
<tr><td colspan="2">Linux layer: camera driver, audio driver</td></tr>
</table>

Figure 1: Android Layer Architecture

The lower most layer of the android is Linux layer that contains all the essential drivers that are needed to communicate with the hardware. The layer above the Linux layer is Library layer. This layer contains various libraries that can be used by developer to handle different type of data. Like Surface manager is used to handle surface of the screen, SSL is used to handle security in web applications.

Next layer is Virtual layer. This layer contains the Dalvik Virtual Machine and basic JAVA libraries. Dalvik Virtual Machine is register based virtual machine which is different from java virtual machine which is stack based virtual machine. All the processes in android are run on this virtual machine. Next is the application framework layer

that contains various application programming interface (API's). This layer manages the basic function of the phone like call management, location management etc.

The upper most layer application layer. This is the layer through which user directly interacts with. All the internal details are hidden from the user. All the application resides in this particular layer. Developers can develop the application and make them available from the play store. These applications can be normal one and malicious one. Any application that wants to use system resources has to take permission from the user. So the permission granting is the whole sole responsibility of the user itself.

There is a need to understand the basic working of android applications, its processes, permission concept and the privacy issues occur with respect to these permissions. Data stored by these applications can be useful for forensic point of view. In android applications data can be stored in 5 locations that is internal memory of the phone, SD card and to the server.

Application like color notes are used by users to store various information like schedule of day, passwords etc. if the information store in these application are accessible by some other application than it is possible for to perform the attack on the user privacy. So to find the impact of these attacks there is a need to understand the storage medium of these applications along with the communication model that they use.

III. Android Application Architecture

In android, application components are basically of four types. Each of which has its own function and life cycle. Android applications use these components in order to perform the required task. One component can access another component and can start the other component in the application.

A. Activities

It represents a single user screen. User communicates with this screen to access the functions of the application. In one application generally more than one activity are available.

B. Service

These are the long running operations that run in the background. It is not visible to the user or it does not provide a user interface. For example, a service may be music player that is running behind another application. Or it may be some process created by the developer to send user personal information to remote server without user knowledge.

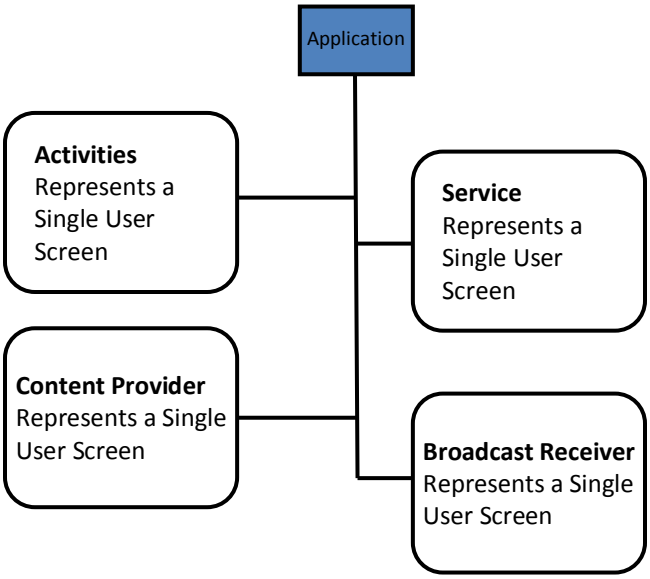

Figure 2: Android Application Component

C. Content Provider

Application data can be shared with the help of content providers. In android application can store their data in SQL files, internal and external storage etc. if one application has to access some other applications data then this can be done with the help of content providers.

D. Broadcast Receiver

These components listen to system-wide broadcast. It can be used to initiate a service when a particular event has been occurred in the phone environment. For example, a broadcast announcing that a particular file has been downloaded into the phone or battery is getting low etc.

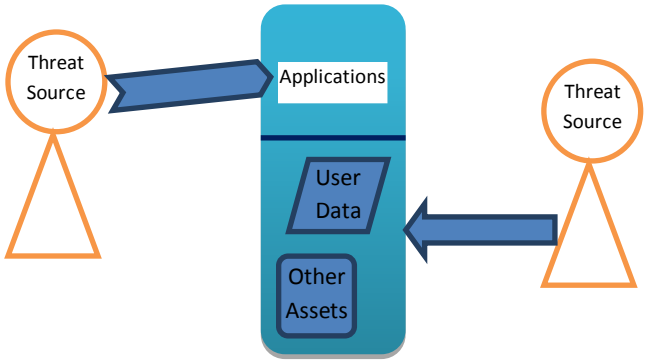

Figure 3: Application Threat Model

IV. Application Threat Model

Application threat model represents the android attack surface through application. That means how the android mobile is under security risk when malicious applications get installed into the phone. Vulnerable applications can also cause harm to user's data.

In the figure 3, threat model has been depicted for the android mobiles. Attack can be performed either on the application itself by exploiting the vulnerabilities of the application or directly attacking the android system. In the case of applications attack, attacker can take the advantage of application vulnerability to retrieve the private information. In the case of operating system attack, dedicated malicious applications are build that supposed to exploit the vulnerability of the existing system.

V. Proposed Work

For the forensics analysis of android applications, first of all vulnerable applications are find out from the android mobile. Attack scenario will be developed and evidences will be collected from the system. The proposed model has been depicted in figure 4. Main modules of the proposed model are as follows:

A. *Retrieved Application*

First of all applications are selected from the android phone and retrieved with the help of android tool. Android ADB (Android Debug Bridge) tool has been used to check what are the application packages installed on the phone then required package has been retrieved and store in the computer for further analysis of the application.

B. *Pre-Processing of Application*

In this phase, android .apk file is converted into the zip file. From this zip file, manifest file has been retrieved. From manifest file, content providers used by the applications are identified.

C. *Analysis of content providers*

For the analysis of the content provider, its properties are checked in the manifest file of the application. If the attribute exported is set true for a particular content provider then this content provider is accessible by other application in the android mobile. After this, with the help of android ADB tool further analysis has been done to check whether the content provider is vulnerable or not.

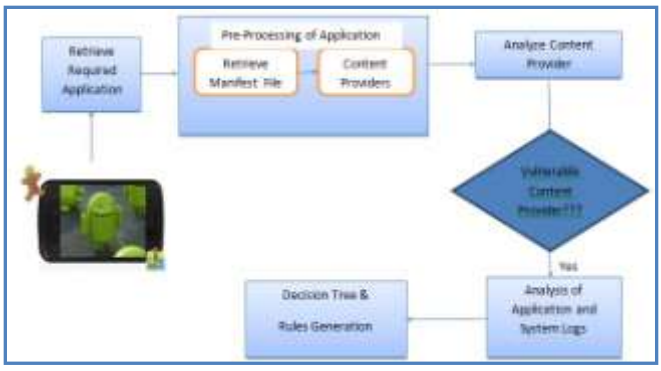

Figure 4: Proposed Model

D. *Analysis of Logs:*

In this phase application and system logs are retrieved from the android mobile with the help of android ADB tool. Then analyze those logs in order to find the evidences of vulnerable applications.

E. *Decision Tree & Rules Generation*

Finally on the basis of collected evidences decision tree has been generated. From the decision tree, association rules are extracted to classify the applications in android mobile.

VI. Conclusion

As the smart phones are becoming more popular, they become the target for potential attacks. To predict where they are moving, it's important to analyze what dynamics are affecting their growth. In this paper, Android architecture, challenges and vulnerability has been analyzed. In future work, more effort can be put into malicious codes detection techniques to help us identify a greater number of security and privacy threats as well as other malicious activities within android applications. Another open problem is the identification of obfuscated malicious activities which have shown to be not easy to detect with static analysis.

Other security problems like inter process communication bugs, botnet using social networking must be addressed. The mobile social network (MSN) concept combines social science and mobile communications and has created a new research area that is relevant for content publishing, data exchange, sharing and delivery services.

REFERENCES

[1.] Android Open Source Project Google, "Android Security Overview", 2011.

[2.] T. Armstrong, "Android malware is on the rise," Kaspersky -2011 [online]. Available: http://www.virusbtn.com/pdf/

conference_slides/2011/Armstrong-Maslennikov-B2011.pdf [Accessed: 4 April 2012].

[3.] W. Enck, M. Ongtang and P. McDaniel, "Understanding android Security" in IEEE Security Privacy, 2009, vol: 7, Issue: 1, pp. 53—54.

[4.] H. Kuzuno, S. Tonami, "Signature Generation for Sensitive Information Leakage in Android Applications" in ICDE Workshops 2013.

[5.] Meghan Kelly "Watch out, Android users: Some web sites are auto-downloading malware to your phone" [Online]. Available: http://venturebeat.com/2012/05/02/malware-drive-by-download-attack/, [Accessed: 15 Feb 2014].

[6.] Kirandeep, Anu Garg "Implementing Security on Android Application" in Int. J. of Engg and Science (IJES) vol: 2, Issue: 3, pp. 56-59, 2013.

[7.] Rohit, "Android Master Key Vulnerability—PoC", [Online]. Available: http://resources.infosecinstitute.com/android-master-key-vulnerability-poc/, [Accessed: 14 Feb 2014].

[8.] "Mobile Threat Report 2011", [Online]. Available: https://www.lookout.com/resources/reports/mobile-threat-report-2011, [Accesses: 10 Feb 2014].

[9.] X. Jiang and Y. Zhou, "Android Malware", Springer Briefs in Computer Science, vol: 3, 2013.

[10.] Jorja Wright, Maurice E. Dawson Jr.and Marwan Omar "Cyber security and mobile threats: the need for anti-virus applications for Smartphone", in JISTP, vol: 5, Issue: 14, 2012, pp. 40-60.