*Available online at*www.scholarsresearchlibrary.com

Scholars Research Library

Archives of Applied Science Research, 2015, 7 (2):34-38
(http://scholarsresearchlibrary.com/archive.html)

ISSN 0975-508X
CODEN (USA) AASRC9

Analysis of advanced issues in mobile security in android operating system

Anjaneyulu G. S. G. N.*, Gayathri M.[1] and Gopinath G.[1]

**SAS, VIT University, Vellore, India*
[1]SITE, VIT University, Vellore, India

ABSTRACT

*Today's era mobile security has become a big issue in day today life. Most of the people want to use smart phones for communication, planning and organizing their schedule for their private life. These technologies are causing profound changes in the organization of information system. Android has been changed in mobile market. Now most of the people are using smart phones for their digital life – email, social networking, important messaging, photo and video sharing and etc. Smartphone are very attractive for users as well as attackers. Most of the attackers are using hacking techniques to get private information about their personal life that is directly generated money for the attackers. It is up to the Smartphone operating system to ensure the security of data in device. In last two years Android became a most popular operating system in the mobile market. For these mobile device is activating over 1.5 million as per day. Android is expected to cross the 1 billion active device barriers in 2013. It covers 70% percent of the mobile market. In this paper we discuss about Android operating system security which has been developed for mobile phones. Android Application development, layered Approach and details of security information for android also an Android Application Sandbox. Which is used for perform both static and dynamic analysis on android programs.***

Keywords: Smartphone, Android OS, layered Approach, Application development, Sandbox.

INTRODUCTION

Android is a new generation mobile operating system which runs on Linux kernel. Android mobile application developed is based on Java Programming. These codes are used to control mobile device via Google–enabled java libraries. It is an Important platform to develop mobile application using software stack provided in the Google Android SDK. Android combines OS features like efficient shared memory, preemptive multi-tasking, Unix User Identifiers (UIDs) and file permission with Java language and its class library. The Security platform is much better than J2ME or Blackberry Platforms. Programs can typically neither read nor write each other's code. The software developers at mobile development India have expertise in developing application based on Android java libraries.

The Android Graphic User Interface (GUI) environment has more secure features in isolation. It is allow application to do some activities like web browser, sending SMS and taking photos. This gives flexibility to the application to use native code without compromise the android's security and it is also give some additional features. Application can also entertain users with graphics like playing games, listing music and Animations. There are many applications are available in android for users according to their usage and everybody can use these application without any permission. It is used to overcome the impact of malware in smart phone.

2. ANDROID PLATFORM SECURITY ARCHITECTURE:

In Android operating system there are 4 layers. Android has its own libraries. This is helpful for developing and designing android applications. These libraries are written in C/C++. Linux kernel is a 1st layer which is also written in C language.

Application Layer: It is the most upper layer in the android architecture of android operating system. All the native application like camera, Google maps, SMS, contacts, browser, calendar, Clock. These applications works with end users with the help of application framework to operate.

Application Framework: Android application which are developing has been needed classes and services. Developers can extends and reuse the components of API, which is already presented. There are managers available which is used for accessing the available applications.

Activity manager: It is a life cycle of applications, which enables to manage all the activities. All the activities in android is controlled by activity manager.

Resource manager: It enables to access data to non-code resource like gaming etc.

Notification manager: It shows the display window to custom alerts in status bar.

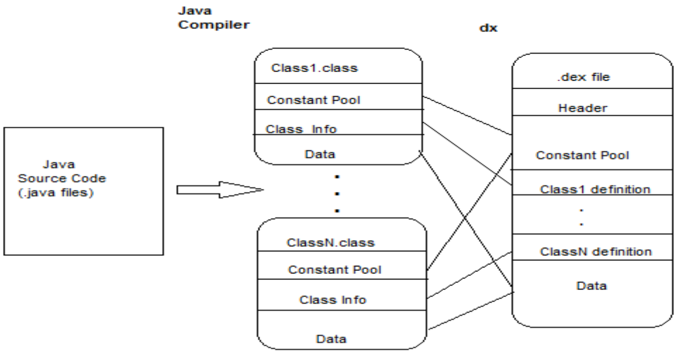
Location manager: It gives alerts when user enter in a specified geographical location.

Package manager: It retrieves the data from installed packages on device.

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

Telephony manager: It works to handle network connection settings and services.

Android runtime: Android has its own virtual machine DVM (Dalvik Virtual Machine), which is enable to execute all the applications. With the help of DVM user can execute multiple application at same time.



Virtual Machine Process

Libraries: Android has its own libraries, which is written in C/C++. These libraries cannot be accessed directly. We need application framework to access the libraries.

There are different types of libraries like web libraries to access web browsers, libraries for android and video formats etc.

3. ANDROID SECURITY CHALLENGES

3.1 Android Platform Security: The security of the platform is depends on a secure boot process. Boot process of an android device is a 5 step process. In which first, CPU starts executing from its reset vector to which the initial boot loader (IBL) code from the ROM. The IBL loads the boot loader from the boot into the RAM and perform a signature check to ensure that is only authenticates code is executed. The boot loader loads the Linux kernel and also perform the signature check. Rooting has been enable to modification in the system partition. Modification in the system partition requires root permission, which is not available by default. There are two ways to get root permission : 1) User boots a custom system that gives him a root shell. 2) User exploits a vulnerability for getting root permission at run time. Unsigned kernel can easily contains malware without any permission and is undetectable by any anti-virus software.

3.2 Android System Security: Since Android 3.0 which is possible to encrypt the data partition with 128 bit AES. It enable file system application files are private. This is owned by that application’s distinct UID. Since Android 4.0 frameworks provides a keychain API in which the user can safely store data and user confidential. The key store is saved at data/misc/key store and each key is stored in its own file. This key is encrypted using 128 bit AES in CBC mode. Each key file contains info header, the initial vector (IV) used for the encryption.

3.3 Android Application Security: In Android application security is based on isolation and permission control. Each application runs on its own process with its own user and group ID which makes it a sandbox. In which application do not talk to each other and do not shared the resources. This isolation is provided by the Linux kernel which is based on UNIX security model of processes and file system permission. Linux mechanism for inter process communication provides a binder framework. Binder is an IPC mechanism and remote method invocation system. Binder contain kernel-level driver and user space system. Binder can call routine in another process and pass the arguments between them. Binder is a very basic security model. Which can identify of communication partners by delivering the PID and UID.

4. EXISTING SYSTEM

Android has two basic methods of security enforcement. In which
a) applications run as Linux processes with their own user IDs and thus are separated from each other. In this vulnerability in one application does not affect other applications. Since Android provides IPC mechanisms, which need to be secured.
b) enforcement mechanism comes into exist. Android implements a reference monitor to access to application components based on permission. If an application tries to access another component, the end user must grant the appropriate permission at installation time.

Android requires that developers declare in a manifest a list of permissions, which the user must accept prior to installing an application. Android uses this permission model to restrict access to advanced or dangerous functionality on the device.

ADVANTAGES AND LIMITATIONS

5.1 Advantages of an Android

- Time for a change.
- Android scales to every device.
- It’s supported by some hardware manufactures and more to come in the future.
- Open source.
- Third party development is encouraged.

5.2 Android has following limitation

- Not supported by any big company yet except HTC.
- Does not support some applications like Firefox.
- Some limitations exist in Blue tooth.

6. LITERATURE SURVEY

Android mobile applications have been widely used in various mobile devices. Android mobile applications are evolving at a meteor pace to given a rich and fast user experience. The increasing order of the hardware and software platforms of mobile devices and promotion of mobile internet have brought a great opportunity to the web application to develop for mobile platforms.

In case of security, Static analysis scans the software for malicious patterns without installing it. Dynamic analysis executes in isolated environment. Ex: Sandbox, which is intervenes and logs low-level interactions with the system for future analysis. Both the sandbox and the detection algorithm can be deployed in cloud providing fast and distributed detection of a suspicious software in a mobile device.

The ultimate goal is to protect the mobile applications from the malicious attributes and safeguard. The internet connection capabilities and complete software platform available in the future web application appears limitless.

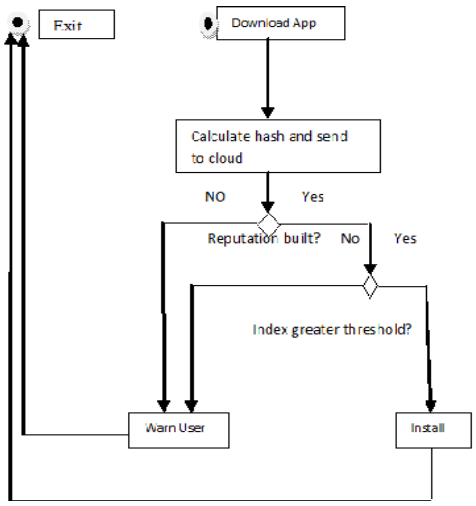
7. PROBLEMS

Most of the attackers can be occurred by the user negligence. Attacks on android devices are trapping in the troubles to the users. And now they are capable of spreading mechanism, which do not require any permission to explicit user confirmation. Malware may be delivered unnoticed through desktop computers, other android devices and some severe virus affects applications. We are using open usage model of android market so malicious applications can easily attacks on user device. Especially pirated application may have severe virus spread to another devices with informing Google as malware.

Google “kill switch” REMOVE_ASSET command will not delete modern malware in future attacks in android are becoming more feasible. USB host mode capable android devices quickly affect the USB debugging enable smart phones. We should make it trivial by the end android-based program, Which is preinstalled on any android 4.0 devices. Also classical desktop malware is severe it makes self-spreading capabilities of android malware. Because of our extensible exploit execution framework, we can find local attacks. Several new and well-known threats apply on smart phones. These include conducting money fraud, corporate and even denial of service attacks on today’s life. Android device may even serve as remote based attacks on other GSM subscribers, through this is regarded highly improbable.

8. PROPOSED SOLUTION

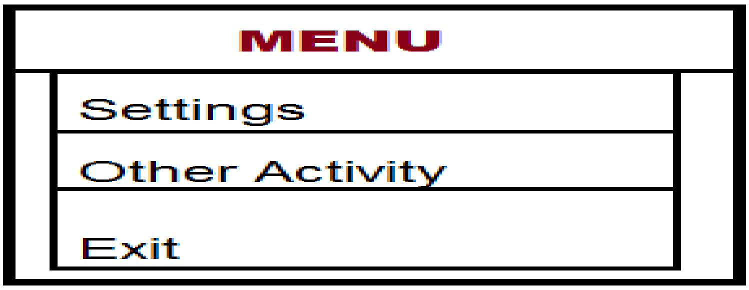
Internet is full of genuine and malicious application. An android user download different types of application from the play store, In this model, it is proposed that after downloading and before installing the mobile device ask the AM cloud for the reputation of the downloaded application.



Based on application behavior and reputation index the downloaded application can be classify in three ways :

1. The application has built a good reputation and there is likely no harm on installing it on the client’s device. Good reputation will be set after some threshold of positive feedback from those clients that have downloaded and installed application in your device.
2. The application has not yet developed any good and or bad reputation in the AM cloud that’s meaning you should be extremely cautions with such an unknown application, the anti-malware provider wish to recommended that the user does not install the application or install the application in the sandbox. Our solution proposes that the anti-malware provider keep track of which unknown applications were installed on which user Android device.
3. The application has bad reputation. In this case, the user is warned about the application bad reputation.

9. ANDROID PROGRAM FOR CREATING MENU



10. ANALYSIS

In 2014 mobile malware development focus on the android platform continuing that we have seen in the last 2 years. They collected sample apps in this they found 14% malicious. What we analyze most of the android apps are affected by the Trojan. Even though they are not fall directly explicitly they sending SMS (e.g., SMS Sender) Almost 83% android were affected by Trojan by sending SMS.

Trojans involved as a silent killer. Data theft, banking fraud are the most common Activity. They found that Trojan affects 10% of android. Backdoors are the common most malware type after Trojan. The Pileup vulnerabilities announced university researchers categorize as a Backdoor, is represented as malware authors to automate creation of Remote Access Trojans) that can secure Google Play Store security.

CONCLUSION

More than 1 million Android devices activated now a days, android has very few restrictions for the developer increases the Security risk for end users. We reviewed that security issues in the Android based Smartphone. The integration of technologies into an application certification process requires overcoming logistical and technical challenges. What our literature survey tells that Android provides more security than other mobile phone platforms. Kirin will help Android into the secure operating system needed for next-generation computing platforms.

REFERENCES

[1] Tiwari Mohini, Srivastava Ashish Kumar and Gupta Nitesh *Research Journal of Computer and Information Technology Sciences* ISSN 2320 – 6527Vol. 1(6), 12-19, November (**2013**)
[2] IJRIT *International Journal of Research in Information Technology*, Vol. 1, Issue 2, February **2013**, Pg. 30-36.
[3] Suhasholla, Mahima M Katti Department of Information Science &Engg. R V College of Engineering Banglore, India, Volume 3 Issue 3, **2012**.
[4]International Journal of IT, *Engineering and Applied Sciences Research* (IJIEASR) ISSN: 2319 – 4413Volume 2, No. 2, February **2013**.