Android based malware propagation and detection in mobile system

S.Anitha[1], S.Giridharan [2], P.Hemalatha[3]
[1]U.G Scholar Department of Information Technology
IFET College of Engineering , Anna University, India.
[2&3]Assistant Professor, Department of Information Technology
IFET College of Engineering , Anna University, India.

---***---

Abstract - ***Now a day's the smartphones have become the most important device for everyone. The smartphone users perform many online tasks including web browsing, Internet banking and share the documents through Internet , SMS services. Currently in the smartphone market, Android is the platform with the highest share. Even in the 21st century where the technology is rapidly growing and simultaneously the increasing use of smartphone has been attracting the attention of malware writers, for these issues the smartphone users are looking for security solutions aimed to develop a android app and also use a slicing mechanism to detect and prevent the mobile malware .and also aims to improvement towards current techniques for better mobile malware detection and detect the virus before enter into the smartphone.***

Key Words: ***Smart phone, Android app, Malware, Mobile Malware Detection and Prevent.***

1. INTRODUCTION

In recent years, the smart phones are worldwide market has grown dramatically. According to CNN smartphone shipments have tripled in the past three years (from 40 million to about 120 million). In a very short time Google's mobile operating system Android has become the number one choice for smartphones. Google's Android contributes to almost 75% of the mobile OS market share [5]. There are three reasons for this famous. Firstly, Android is Open Source. This open source code and permissive licensing allows the software to be freely modified and distributed by device manufacturers, wireless carriers and enthusiast developers. Secondly, Android is free. Android, since the day it was launched, has been available free of cost and Google made it clear so that it will be a free in future. The OS caught the attention of manufacturers across the world and many initially adopted it for low cost smart phones. Thirdly, Android Market created an possibility for tens of millions of software developers around the world to reveal their skills and come up with new packages for Android telephones. Its users have a huge sort of packages to choose from and can customize their phones for a private revel in. The Android working gadget has been at the upward thrust with the increase malware hazard for mobile phones functionality As the maximum popular cellular platform, Google's Android overtook others to emerge as the pinnacle cell malware platform. It has been highlighted that "among all cell malware, the proportion of Android-based malware is better than forty six% and nonetheless developing unexpectedly." [6] Another recent file also alerts that there's "400 percentage boom in Android-primarily based malware in view that solstice 2010". Given the wild boom of Android malware, there may be a pressing need to successfully mitigate or guard in opposition to them. For this, the android circle of relatives is characterized based on their precise conduct breakdown, along with the set up, activation, and payloads. To cater to this, a dataset of forty nine families of android malware, discovered from Aug 2010 to Sept 2011[1], had been considered. However, without an insightful expertise of the android's underlying framework and its safety mechanisms, it's far tough to imagine an effective mitigation solution may be practically evolved.

2. MALWARE

The malware are termed as malicious software this is designed especially to target a cell device gadget, such as a tablet or smartphone to harm or disrupt the tool. The maximum cellular malware is designed to disable a cellular device, allow a malicious consumer to remotely control the device or to souse borrow non-public facts saved on the device .Once malware gets itself into the device through different media like copying of documents from outside devices onto the device and by and large by downloading files from the net, it assessments the vulnerabilities of the machine and infects the machine if the device is quite susceptible or not. The concern for the rate of unfold of malware nowadays is a worldwide phenomenon, especially it spreading double over the net that is a method of world conversation. Today's malware is capable of doing many things, inclusive of: stealing and transmitting the contact list and other statistics, locking the device absolutely, giving far flung get right of entry to to criminals, sending SMS and MMS messages thru Bluetooth and net. Mobile malware reasons severe public issue as the population of mobile phones is lots larger than the populace of Personal computer systems.

3. MOTIVES TO CREATE MOBILE MALWARE

3.1 Novelty and Amusement:-Some malware causes mischief or damage in a way that appears to be intended to amuse the author. For example, I keep. Changed The wallpaper of infected phone devices, and sent anti religion textual content messages from Android phones. Many portions of malware fall into this category and no other

3.2 Selling User Information:-Mobile running machine APIs offers the packages with huge amounts of Information approximately the customers. Applications can query cellular APIs for the person's vicinity, listing of contacts, browser and down load history, listing of established packages, and IMEI (the specific device identifier). Although we can't realize positive why malware collects this data, we hypothesize that this information is being sold by means of malware vendors for monetary gain.

3.3 Stealing User Credentials:-Credentials may want to Be used directly through malware authors for extra Financial Gain, however financial fraud may be hard to Perpetrate and requires specialization. People use Smartphone's for shopping, banking, email, and Other Activities that require passwords Other Activities that require passwords and charge Information. Banks rely upon cellular phones for two-factor Authentication. Users may keep authentication And fee credentials in text files on their Phones (as an instance, to use the phone as a mobile Password manager). This makes cell phones a target For credential theft. Three pieces of malware in our Data set target user credentials by intercepting SMS Messages to capture bank account credentials.

3.4 Premium-Rate Calls and SMS:-Legitimate premium-rate phone calls and SMS messages deliver valuable Content material, inclusive of inventory fees, technical support, or grownup offerings. The price of a top rate- charge call or SMS is charged to the sender's cell phone bill. Premium price calls can cost several dollars in line with minute, and top class-fee SMS messages can fee numerous bucks consistent with message. In Android and Symbian.

4.EXISTING SYSTEM

Previous researchers have proposed some of models, methods, and mechanisms to detect and prevent malware in cellular gadgets .The Existing research on computerized vulnerability discovery for packages ("apps") usually makes a specialty of numerous unique forms of vulnerabilities because of the decidability of the established problem of spotting application vulnerabilities.

For instance, ComDroid aims at Intent related problems (that is, unauthorized Intent receipt and Intent spoofing), SMV-Hunter detects SSL and Transport Layer Security (TLS) man-in-the-middle vulnerabilities, Content Scope examines the vulnerabilities of an unprotected content company, Android Leaks uncovers capacity personal information leakage, Woodpecker objectives functionality leak vulnerabilities, CHEX discovers factor hijacking vulnerabilities.

However, those systems effectiveness and performance are typically limited in exercise because of the exponential boom of paths to observe, simplified assumptions, and the limited number of vulnerability styles.1,8 Moreover, it isn't clean to extend those systems to seize new vulnerabilities, despite the fact that they share some not unusual, components (which include building manage-glide graphs and dataflow graphs).

5.DISADVANTAGES

It is not easy to extend these systems to capture new vulnerabilities, although they share some common, components (such as constructing control-flow graphs and dataflow graphs).They did not Discover vulnerable apps, and it is not clear how SCA processes those apps.

6.PROPOSED SYSTEM

A new static-evaluation framework to facilitate vulnerability discovery for apps by means of extracting detailed and precise information from apps and easy for the identification process. Moreover, the framework can decrease the manual-verification capacity by performing slicing and filtering out infeasible paths. To our information, existing approaches cannot achieve these goals simultaneously. Moreover, defining app property graphs (APGs) and using graph databases can scale up the vulnerability discovery process. finding potential vulnerabilities is turned into performing graph traversals over CPGs with much better performance in terms of accuracy and flexibility. While we also model vulnerabilities as graph traversals and conduct graph traversals to find vulnerable apps, significant changes exist between the two approaches.

7. PROPOSED SYSTEM ADVANTAGES

The Proposed system are used to avoid Data drip, Reliable, High data transmission rate Avoid replicate request.

8. PROPOSED SYSTEM ARCHITECTURE

The Android application structure with focus on its main files folders This account will serve as preliminary knowledge in understanding Apps in Android based mobile platform ,through which our algorithm can extract useful pattern for malware detection .Android uses several partitions (including boot ,system, recovery, data etc.)to establish files and folders in the device with every partition having its Of functionality.

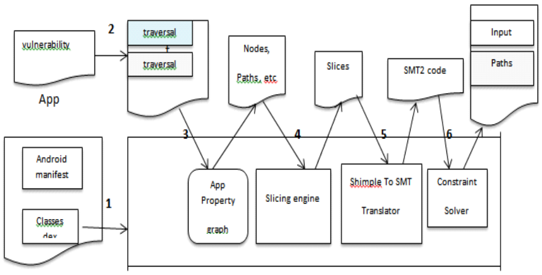

Fig-1:over view of architecture

The Architecture of Android consists of the following:

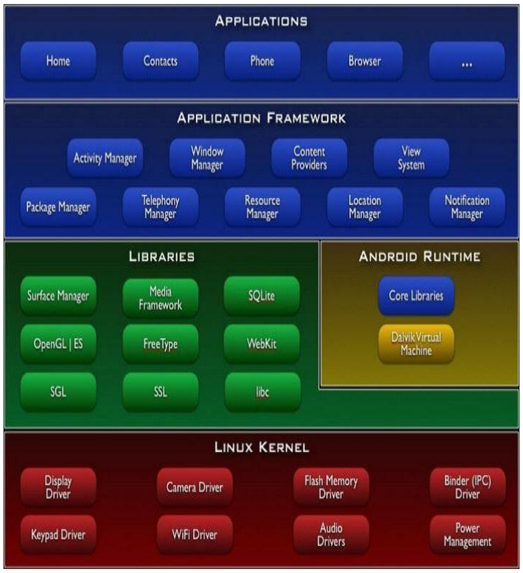

Fig.2 android app

8.1 Android security:

Android provides two main security mechanisms that are different from traditional Unix structures, i.e., application sandboxing and permissions.

8.2 Sandboxing: Sandbox is an isolated environment For the implementation of an application. Each app has its own Sandbox which contains app's data and code. This is Implemented by giving each Android application (*.apk) its own exclusive UID at mount time that remains stable throughout its period.

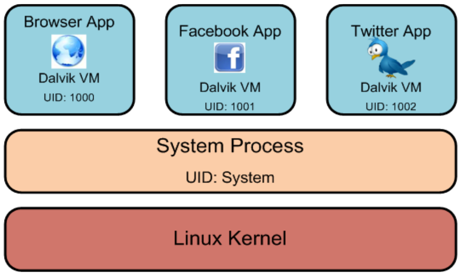

Fig 3sandboxing

8.3 Permissions: Presentation permissions is a Mandatory Access Control (MAC) mechanism for protective application components and data. In its simplest form, access to each component is limited by allocating it an access permission label; this text string need not be exclusive.

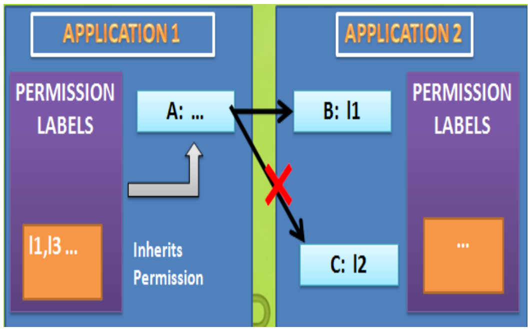

Fig.4permission

9. PROPOSED SYSTEM METHODOLOGY

i. Determining components of interest
ii. Producing Fault Injected Apps
iii. Determining Differential Analysis
iv. Prototype Implementation

9.1DETERMINING COMPONENTS OF INTEREST

The first step in the analysis of an app is detecting components of importance (Co Is), i.e. if it does not fit a model M(c) defined for all components Of kind (c).

In current model of ALTERDROID, fashions measure statistical functions simplest, such

as for example the expected entropy, the byte sharing, or the average size. Such features are computed from a dataset of modules of the same type, such as writing files, pictures, code, etc. For each model M, I assume a Boolean function test (cM) that returns true If c complies with M, and false otherwise.

9.2PRODUCING FAULT INJECTED APPS

Components of interests famous in the previous stage are injected with faults and reassembled, together with the remaining app modules, to generate a faulty app P.

This process can generate Several fault-injected apps, as there are a couple of approaches of applying unique FIOs to one of a kind components within the set of Co Into different components in the set of Co Is.

In ALTERDROID, fault-injected apps are created one at a time and sent for difference analysis.

If no evidence of malicious behavior is found in the differential analysis, the fault injection process is invoked again to produce a different faulty app, and so on.

9.3DETERMINING

DIFFERENTIAL ANALYSIS

Differential analysis between a candidate fault-injected app and the unique app is carried out behind the model.

The process comprises the following steps: Make an proper usage form and con-text t, to feed together apps and extract their behavioral signatures. Both the original and the fault-injected app is tested under the same conditions and using the same inputs. Note that this assumes that the finishing of an app is fully deterministic

9.4 PROTOTYPE IMPLEMENTATION

ALTERDROID is applied using Java and relies on a number of Android open source tools for specific tasks. App modules are extracted using Android. After fault injection, modules are repackaged into a modified app using Apk Tool. Monkey is used to generate a common classification of events to interact with both the original app and the fault-injected app. These events should be produced specifically for each test to intelligently drive the GUI exploration, i.e., to test code applying different functionalities of the app.discourage malicious apps like creating a centralized market place. The coarse grained Android permission model can possibly be expanded to include additional context material and to better facilitate users to male sound and informed decisions. Unique runtime environment, with limited resources and battery prove to be a hindrance in the deployment of sophisticated detection technique. Prompt development and increased sophistication are posing significant challenges for their detection. Studies show that the best case detection by mobile antivirus is 79.6% and worst case is only 20.2%.thus, The main contribution of th Proposed solution is to supply a brand new model, technique and method to hit upon and prevent malware rough a alignment of static analysis and vulnerability-discovery methodology.

10.CONCLUSION

The various methods by which Android apps are diseased with malware have been studied in detail. We have seen the ingenious methods using which the infected apps are installed. A large volume of new apps are created on a daily basis. Therefore, a joint effort involving all parties in the ecosystem is needed to spot and discourage malicious apps like creating a centralized market place. The coarse grained Android permission model can possibly be expanded to include additional context information and to better facilitate users to male sound and informed decisions. Unique runtime environment, with limited resources and battery prove to be a hindrance in the deployment of sophisticated detection technique. Rapid development and increased sophistication are posing important tasks for their detection. Educations show that the best case detection by mobile antivirus is 79.6% and worst case is only 20.2%.thus, The main involvement of the suggested result is to produce a new model, method and technique to detect and prevent malware through a combination of static analysis and vulnerability-discovery approach.

REFERENCES

[1] Yawing Zhou, Xinxiang Jiang "Dissecting Android Malware: Characterization and Evolution" in 2012 IEEE Symposium on Security and Privacy.

[2] Amiga K. Maji, Farad A. Arshad, Saurabh Bagchi "An Empirical Study of the Robustness of Inter-component Communication in Android"

[3] Ariel Haneyy, Erika Chin, David Wagner, Adrienne Porter Felt, Elizabeth Hay, Serge Egelman "Android Permissions: User Attention, Comprehension, and Behavior".

[4] (2011) Smartphone Shipments Tripled Since '08. Dumb Phones Are Flat.

[5] http://tech.fortune.cnn.com/2011/11/01/smartphone-shipments-tripled-since-08-dumb-phones-areflat.

[6] (2012) Android beats iOS 5-to-1 in Q3 smartfone market share. http://news.cnet.com/8301-1035_3-57544131-94/android-beats-ios-5-to-1-in-q3-smartphone-market-share.

[7] Malicious Mobile Threats Report 2010/2011.http://www.juniper.net/us/en/company/press-center/presreleases/2011/pr 2011 05 10-09 00.html.

[8] Developer.android.com

[9] Repackaged application leaks your smartphone information http://en-erteam.nprotect.com/2011/07/material-repackaged-fastracing-game 8549.html

[10] QR code. http://en.wikipedia.org/wiki/QR code.