Malicious apps Detection by Integrated Approach of Signature, Permission and Feedback Method in Android OS by using Mobile Network

Chetan J. Shelke,
Asst. Professor, Dept.of IT, P.R.Patil College of Engineering, Amravati, India

Abstract- Malware is the most serious threats now a days many attack were launched using open platform android With the increasing significance of malware in Internet attacks, Thus developing malware detection approach that is both *effective* and *efficient*, and thus, can be used to replace or complement traditional malware detection methods by using signature, permission as well user feedback methods.

Keywords- malware, filter, signature.

I. INTRODUCTION

Smart phones are steadily gaining popularity, creating new application areas as their capabilities increase in terms of computational power, sensors and communication. Emerging new features of mobile devices give opportunity to new threats. Android is one of the newer operating systems targeting smartphones. While being based on a Linux kernel, Android has unique properties and specific limitations due to its mobile nature. This makes it harder to detect and react upon malware attacks if using conventional techniques.

To overcome the drawback of existing system this proposed work proposes a new approach which is able to perform both static and dynamic analysis on Android programs to automatically detect suspicious applications. Static analysis scans the soft-ware for malicious patterns. Dynamic analysis executes the application in a fully isolated environment, which intervenes and logs low-level interactions with the system for further analysis. The algorithm can be deployed inthe mobile network, providing a fast and distributed detection of suspicious software in a mobile software store akin to Google’s Android Market. Additionally, System might be used to improve the efficiency of classical security applications available for the Android operating system.

In present system secured framework against application installation attacks on mobile network platform. Present system applied parallel processing of three approaches i.e user feedback filter, signature based detection filter and permission based filter. After using all the filter that is filter1 ,filter2 ,and filter 3 proposed system combined the result of all the filter and find out the probability that particular application is malicious or not. This system use RJ48 tree based decision system to find out the probability of malware

This proposed system proves to be efficient for the user those who are downloading app from unknown sources . The research work will also focus on overcoming the problem of various attacks on mobile Smartphoneplatform. The proposed methodology storing the data of permission, signature and feedback of malicious app on mobile network so that less storage space required on mobile phones.

II. LITERATURE REVIEW

Static analysis techniques rely on examining the binary code to determine its properties without actually executing it.There are two types of methods of static analysis depending on the features utilized for operation: statistical and graph matching-based methods. In the statistical method, defenders transform the binary code of malware into an assembly code to extract and analyze characteristics[1,2], such as the n-grams of instruction or call patterns. The graph matching method is mainly based on similarity matching. For that, defenders build call graphs (e.g., system call graph, function-call graph, or API call graph), compare graphs with each other, and classify malware based on how well defenders match with previously known behaviors of the given malwares pieces. Using polymorphism or metamorphism techniques, malware can disguise its appearance while keeping its behavior unchanged. As a result, such techniques using signaturebased methods are easily evaded by cyber criminal

Dynamic Analysis. Dynamic analysis approaches runexecutables inside the isolated environment to capture the runtime behavior.These approaches extract behavioral characteristics through taint analysis on the relation of systemor API caller-callee. This approach addresses obfuscation, packing attempts, and self-modification[3,4,5]

III. PROPOSED METHODOLOGY

With the highly emerging use of smart phones .smart phones now a days able to perform various task as the cashless services are increasing day by day sensitive application such as banking related app rising danger due to malware attack its quite difficult and challenge to detect new malware In this article we present secured framework against application installation attacks on mobile network platform in this we applied parallel processing of three approaches i.e. user feedback filter,signature based detection filter and permission based filter.This system use j48 algorithm to find the app is malicious,non malicious or suspicious.

Steps of Algorithm for theProposed System

Step A: For Signature Based Detection,

Step i: Extract signature from app .

Step ii: Submit the extracted signature to the mobile network

Step iii: Match the extracted signature with malicious signature database

Step iv: Calculate the malicious and non malicious percentage ratio.

Step v: Generate match Score to each app in each IMEI.

Step vi: Notify the user about maliciousness about the app.

Step vii: If the application is not found as malicious by signature based detection go to step 2

Step B: For Permission Based detection, apply K-means clustering Algorithm to sort the application is malicious OR not

Step i: Extract permission from android.xml file .

Step ii: Submit the extracted permission to the mobile network

Step iii: Match the extracted permission with malicious and non malicious permission cluster.

Step iv: Calculate the malicious and non malicious percentage ratio.

Step v: Generate match Score to each app in each IMEI.

Step vi: Forward the score to step 3 i.e user feedback method for further analysis.

Step C: For User feedback method**,** user gives the user feedback about installed app.

Step i: Top n results are retrieved or extracted from the user.

Step ii: Submit the extracted feedback to mobile network

Step iii: Pre-process the feedback i.e positive and negative find out the score of particular app for each IMEI

Step iv: classify the application as malicious,non malicious,suspicious by using decision tree based classification i.e J48 algorithm

Step v: notify the user about maliciousness about the app

Proposed system firstly match the signature with signature database if the signature is not match then application will check with permission as well as user feedback method by using RJ48 method

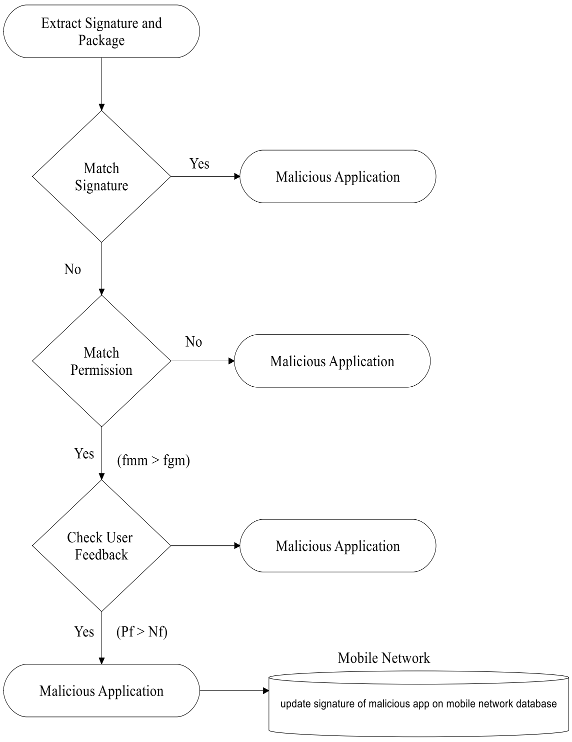


Fig.1: System flow of proposed system

Approach

1. Extract Signature of Application(//sign from user level component)

if (sign = = matching sign from DB (//at mobile network component){

Declare Application as malicious

} else {

Go to Step 2

}

2. Extract Permission of Application (//from user level component per IMEI)

3. Determine fgm ,fmm

4. If(fmm > fgm)

Go to step 5

Else

Go to next application and repeat above procedure

5. Check for the user feedback of application pf and pn (//from mobile network component)

6. If (nf > pf){

Declare Application as malicious

Else

Go to next application

7. Exit.

Where fgm = Permission match factor with genuine matching,

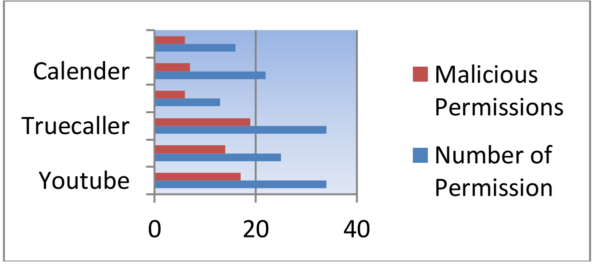
fmm = Permission match factor with malicious matching ,

pf= positive feedback & nf = negative feedback

As the step stated in approach of proposed system firstly all metadata are extracted from user level component i.e user feedback, permissions, and signature once the metadata is extracted ,the extracted data is sent over the mobile network where the processing of signature based detection,permission based detection and user feedback method will be done and after analysis user will notify about malicious or non maliciousness about the application.

IV. RESULT ANALYSIS

From the result of permission based detection and user feedback method decision is calculated by decision based tree J48 algorithm stated in proposed algorithm as in case of skype application both method that is the user feedback method and permission based detection gives the result as non malicious so according to the algorithm the result is non malicious



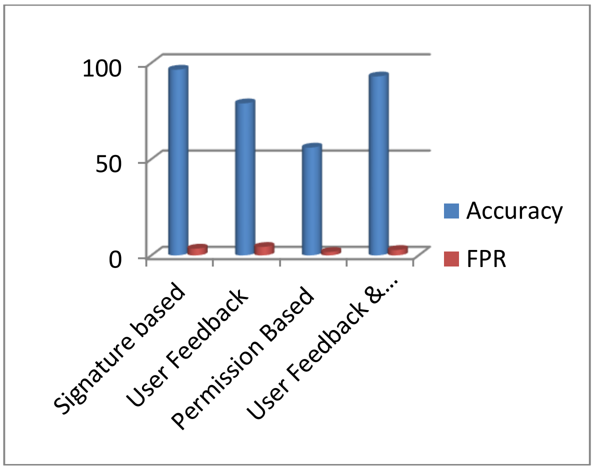
Graph 1 shows the example of total number of permission and comparative analysis of malicious permission taken as per the permission based detection here the app FM, Colander, Telephony, jio and you tube are non malicious as they take less than 50 % ration of malicious permission and the app truecaller take more than 50%.so as per the permission based detection the application is malicious. As signature of true caller is not present in malicious signature set then the result of true caller is non malicious by signature based detection. also the system check for user feedback method the current analysis for true caller as per user feedback method is non malicious.The result of decision based tree j48 algo is suspicious

Malicious+non malicious=suspicious

Few test performed on implemented system by using 25 malicious app and 100 benign application on the mobile network and found that accuracy is not certain i.e. it differ by different application.

TABLE 1 ACCURACY FOR SIGNATURE,USER FEEDBACK,PERMISSION METHODS

Sr. No.	Method	Accuracy	FPR
1	Signature based Detection	96.5 %	3.5 %
2	User feedback method	79 %	21 %
3	Permission based detection	56 %	44 %
4	User feedback &Permission based detection	93 %	7 %



Graph 2 :analysis of signature,permission,user feedback method

$$AF = \frac{\text{Signature based} + \text{User feedback} \,\&\, \textit{Permission based detection}}{2}$$

$$Accuracy factor = \frac{96.5 + 93}{2}$$

$$Accuracy factor = \frac{189.5}{2}$$

$$\therefore Accuracy factor = 94.75$$

V. CONCLUSION

As Smartphone's devices are being rapidly utilized by enterprises, and various government agencies also in military services, security plays an important role, because many users uses these devices to hold their valuable sensitive data, attackers may use this sensitive information with wrong intent. Mobile malwarees can cause many types of damages like, private data leakage, remote listening etc. also they can congest the servers by sending many unwanted messages and spam's and reduces the efficiency of communication network. Hence in order to control these malware attacks in Smartphone's some crucial steps must be taken to provide some efficient mechanism for controlling the growth and productions of these malwares. The extensive use of virtualization in implementing mobile network infrastructure brings unique security concerns for customers or tenants of a public mobile network service. A number of works have investigated these weaknesses from various perspectives, including demonstrating how applications can communicate through covert channels, developing tools to detect information leaks, and implementing more powerful protection mechanisms. Providing better security policies is becoming most important area of research.

VI. REFERENCES

[1]. Rohit Kale Prof. P D. Lambhate " Malware security for Android Components using Layer permission" International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 5.

[2]. Dhavalkumar K. Baraiya1 Prof. Hiteishi Diwanji "Enhanced Permission based Scheme for Android Malware Detection"

IJSRD - International Journal for Scientific Research & Development| Vol. 3, Issue 04, 2015 | ISSN (online): 2321-0613

[3]. Iker Burguera, Urko Zurutuza, and Simin N. Tehrani." Crowdroid: behavior-based malware detection system for Android", In Proceedings of the 1st ACM workshop on Security and privacy in smartphones mobile devices, SPSM '11, pages 15–26, New York, NY, USA, October 2011. ACM.

[4]. J. Chow, T. Garfinkel, and P. M. Chen. "Decoupling dynamic program analysis from execution in virtual environments",In Proc. of USENIX'08, 2008.

[5]. Sven Bugiel, Lucas Davi, Alexandra Dmitrienko, Thomas Fischer, and Ahmad-Reza Sadeghi. Xmandroid: *A new android evolution to mitigate privilege escalation attacks.* Technical report, Technische Universit¨at Darmstadt, 2011.

[6]. Eric Y. Chen and Mistutaka Itoh. "Virtual smartphone over ip", In Proceedings of the 2010 IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2010.

[7]. David Dagon, Tom Martin, and Thad Starner. Mobile phones as computing devices: The viruses are coming! IEEE Pervasive Computing, 3:11-15, October 2004.

[8]. "Cabir-Smartphone Malware" Available: http://www.f-secure.com/v-descs/cabir.shtml [Online, Access: 15 December 2014]

[9]. Smalley S. and Craig R., Security Enhanced (SE) Android, Available: www.Internetsociety.org/sites/default/files/02_4.pdf.[Online, Access: 20 Jan 2015]