International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - NCSCT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
March, 2018 | Available Online at www.ijeecse.com

Review Paper on Sensor Based Application for Malware Detection in Android OS (Operating System) Devices

Shazia Haque[1], Monali Barua[2]
[1]Associate Professor, [2]UG Scholar, Department of Information Technology, Poornima College of Engineering, Jaipur
[1]shazia@poornima.org, [2]2014pceitmonali@poornima.org

Abstract: This paper is the review of the selected research paper which proposes the solution of a major problem of malicious applications in Android. In today's world, around 81.7% of the people are Android users. So as the numbers of users are increasing, the numbers of malicious applications are also increasing which are degrading the security of the devices. The existing anti malwares cannot detect the malware once it changes its form. To overcome this problem, a technique is proposed using SVM (Support Vector Machine) tool.

I. INTRODUCTION

The anti malwares of today's world have a certain standard when it comes to detect malwares. But they lack at certain places when the malware changes its form and comes back again. The tools like virus detectors and scanners look for the byte sequence to detect the malicious codes. .The strength or quality of a detector is based on the concept or technique used for detection. A malware detector is said to be the best if it can detect the virus in its any form (original or obfuscation form) and must be able to detect the unknown malwares as well.

The commercial malware techniques are not very strong to identify the newer attacks on the phone of the user as malware writers always update the threats to overcome the detector software. The Application Paser will extract the types and names of its components and for Broadcast Receivers and it also extracts the registration modes like static or dynamic.

Afterwards, Parser will showcase ICC (Inter Component Communication) related features in the below format: component name (activity/service/provider). The Parser will hold the number of external explicit intents. It is very essential to measure the target of the explicit intent which includes both internal and external components. Each and every android application communicates to each other through ICC- Inter-Component Communication.

This makes the whole case worse because then the malwares can take advantage of the scenario and they performs obfuscate malicious behavior in the ICC to bypass the detection method. In such cases, it becomes very difficult to detect the malwares and the ICC information has to be analyzed thoroughly to detect the malware in this case.

Now, there is an ICC Detector which examines the ICC patterns and also studies the communication patterns between the application and the android system and it also studies the interaction among the applications. Hence, ICC Detector helps in detecting the advanced malwares which bypasses several antimalware prototypes and mainly helps in detecting the malwares dynamically.

II. OBJECTIVE OF THE PAPER

A. Objective:

This research proposes a unique method to detect malicious applications called SVM. The technique includes checking the application on many different levels and attributes like analysis of suspicious API calls, analyze signature, filtered intents and permissions to analyze, sensors to classify an application etc.

It analyzes all the major components of an application before notifying it to the user. This research paper also includes the behavior based detection method which helps in getting rid of the signature method. The main disadvantages of Signature based method is :

i) It requires high space usage (basically large database of malware signature).

ii) The antimalware needs to be updated frequently.

B. About:

- The paper uses Static Analysis method in which permissions are requested and filtered intents are extracted from the Android Manifest file.
- The paper also eliminates the use of signature base method because of the two huge disadvantages like large storage space and malwares need to be updated frequently.
- The tool which is used for the Static Analysis for malware detection is called Smali.
- The proposed work in this paper also tests the Android sensors.
- The SVM uses a combination of kernel to work for better results.

III. RELATED WORK

Manifest files are the main object for all the android applications. Hence, this method can be applied to all android applications and tools. The results of the simulation shows that the method which has been proposed can identify unknown and harmful malwares which was a tough task for the simple signature-based approach.[1]

After all the research and test works, the cost involved in this method is also cheaper as the people who proposed the work used only the manifest files to be detected for malware. 365 samples were evaluated.[2] They implemented a method which is robust and lightweight android malware installation. The work is done thoroughly by them which include extraction of all relevant and detailed features to malware behavior captured at different API levels.[3]

The main purpose of this paper work is to give a focus on attaining a very efficient and smart system for android platform and it also aim for systemizing the android malware. When the researchers performed a comparative study of four different representatives mobile security software, the results of the experiment showed that the method gained 79.6% success rate and 20.2% failure rate. Hence, the result of the experiment clearly states that the proposed method is open for any kind of improvement for the next-generation of automobile malware solutions.[4]

Another proposed work was given a chance to change the face of the malware detection applications. It is called DREBIN. is a proposed method which is lightweight and robust for android malware detection. This can be implemented directly on any android device. DREBIN performs a depth static analysis on many features of an application and stores them in the form of vectors in a vector space.[5] During the former one the application can be put at risk by malicious activity, service launches, and broadcast injection. Hence to prevent the application from these attacks we have introduced a tool called ComDroid to detect and prevent these vulnerabilities. ComDroid is based on DEX code where the Android market can use to evaluate an application even if the source.

IV. PROPOSED WORK

A traditional android application will consist of four components: Service, Activity, Content Provider and Broadcast Receiver. Usually all the four components are taken into consideration for ICC detection. Malwares can send the malicious Implicit Intents to the benign application through exposed components. Usually these components are used to receive the internal implicit intents which are not recommended in Android due to some security reasons.

In this paper we propose a static analysis method by using suspicious API calls, analyze signature, filtered intents and permissions to analyze, sensors to classify an application as benign or malware. The requested permissions and filtered intents are extracted from the Android manifest xml.

Most of the methods available use signature based anti malwares and the signature has to be updated for all the malware updates. The users need to update their antimalware's every now and then and this occupies a huge space in the memory. Disadvantages of using signature based method are:

1. The antimalware has to be updated frequently.

2. Usage of high space (large database of malware signature). The system architecture is shown in the Fig. I. In this paper the behavior based detection method is introduced which helps in getting rid of the signature method.

The two main vastly used methods for malware application analysis are: Static analysis and dynamic analysis. Static analysis: This method will statically analyze features like application components, permissions, interfaces like broadcast receivers, activities, services, etc. This method will not run during the run time of the application and it analysis the flow and data, logical structure and so on.

Smali is the tool to perform static analysis which is an open source tool for static analysis. Dynamic analysis: This method analysis the features at run time to check for malicious behaviors. It monitors the application dynamically in a protected environment and event based environment. But the challenge with this approach is that it cannot be implemented on mobile devices like phones because they can damage the device and destroy information.

It can be implemented only in controlled environment. It is mostly used when large volume of applications is used and checks malware binary at run time. It is highly efficient than the static method and can be applied for offline detection as well. .Fig.II gives the flow diagram of the proposed work.

The malicious behavior in an application happens due to these series of sensitive APIs at high risk levels. These sensitive APIs are selected from Android SDK and numbered and hence those troublesome malicious behaviors can be ruled out effectively using this approach.

Our new approach is based on a modified version of the Stock android Keyword and other modules to support the system called the sensorkeystroke dynamics techniques for authentication purposes. In this method the user needs to enter a fixed-text password which is then immediately processed using the authentication system for analysis.

The prototype will record all the interaction between the user and the application by capturing the key-press events and sample movement sensor data from the accelerometer and the gyroscope. The following android sensor sampling interfaces are used in the proposed system: Type_Linear_Acceleration and Type_Gyroscope. It helps in collecting sensor values at high speed or high sampling frequency.Sensor_Delay_fastest flag is used at the sensor listener registration time.

Fig. 1. System Architecture

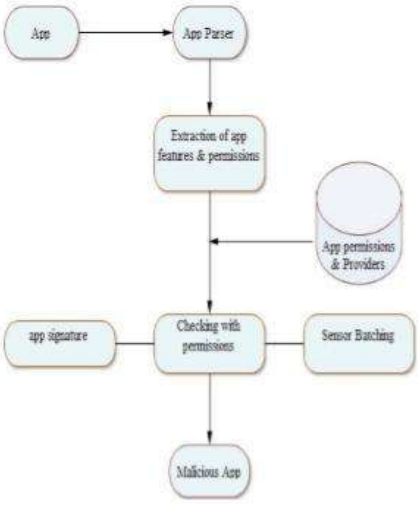

Fig. II. Proposed Flow Diagram

V. METHODOLOGY

SVM (Support Vector Machine):

SVM (Support Vector Machines) is basically used for the classification of data. It is proposed to be better than the existing systems like Neural Networks system because it gives some unsatisfactory results and incorrect outputs at instances. The SVM method needs two processes: training and testing set of data.

Each and every instance included in the training set will contain a single target and several attributes related to it. SVM also performs well and give good results in pattern classification problems. When we apply SVM as a solution to a problem, there are various other components of the SVM which are to be considered for it to be an effective solution to the problems that arises.

One of the main aspects of the SVM is the process of choosing the right kernel for the given application. Out of all the possible combinations of the kernels, Gaussian kernel and Polynomial kernel are the most commonly used kernels but if the given set of data has discrete structure, then a more elaborated kernel will be needed for the SVM. If the kernel and optimization criterion are made right then the system is almost in place for action. When working with dynamic model the traditional methods can fail due to the high dimensionality of the data, but SVM can help in removing this drawback.

The approach used for text classification can also be used for image classification using the case linear hard margin machines to generalize it. SVM is used in the proposed method for data classification where the stored files are in a variety of format and it needs to be classified into groups.

VI. CONCLUSION

The whole gist of the research paper is that the traditional methods of malware detections are simply based on the permission features which become useless because it cannot identify the malwares in its obfuscation state. In this paper, a review has been done on the proposed work which includes an efficient method which combines several features to analyze a malware activity. Sensors, encryption model and permission features are used for the main functioning in this proposed method.

This method also increases the detection rate of malwares and can detect malwares which are in their obfuscations state as well. By monitoring the API calls, permissions it becomes very easy to detect the malware with all the more accuracy.

VII. REFERENCES

[1] Ryo Sato, DaikiChiba and Shigeki Goto, “Detecting Android Malware by Analyzing Manifest Files” 2013.

[2] YousraAafer, Wenliang Du, and Heng Yin "Droid API Miner: Mining API-Level Features for Robust Malware Detection in Android" 2013.

[3] Yajin Zhou, Xuxian Jiang" Dissecting Android Malware: Characterization and Evolution" Sep 7, 2011.

[4] Daniel Arp, Michael Spreitzenbarth, Malte H¨ubner, Hugo Gascon, Konrad Rieck1 "DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket" Feb 23, 2014.

[5] Erika Chin Adrienne Porter Felt Kate Greenwood David Wagner "Analyzing Inter Application Communication in Android" July 1, 2011.

[6] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, David Wagner" Android Permissions Demystified" Oct 17, 2011.

[7] Lucas Davi, Alexandra Dmitrienko?, Ahmad-Reza Sadeghi, Marcel Winandy "Privilege Escalation Attacks on Android" Oct 25, 2010.

[8] ShobhaVenkataraman, Avrim Blum, Dawn Song "Limits of Learning-based Signature Generation with Adversaries" Oct 21, 2011.

[9] Chao Yang, ZhaoyanXu, GuofeiGu ,Vinod Yegneswaran, Phillip Porras "Droid Miner: Automated Mining and Characterization of Fine-grained Malicious Behaviors in Android Applications" April 2012.

[10] Michael Grace ,Yajin Zhou , Qiang Zhang , ShihongZou , Xuxian Jiang "RiskRanker: Scalable and Accurate Zero-day AndroidMalware Detection" June 2012.