Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 04, April-2020

A Survey on Permission based Malware Detection in Android Applications

Sunali Jogsan
ME Student
Gujarat Technological University
Ahmadabad, Gujarat, India

***Abstract*---The android operating system is basically for mobiles and is quickly gaining the market share, where most of the smartphones and tablets either released or set to be released. Nowadays Android application is widely used by the users and performs many different types of activities. So the android platform has become a primary target of attackers. In the world of technology, there are much malicious application reported and performing malware activities which are not matching with their expected behaviors. So detecting the malicious android application is a must. This paper is about the identify the malicious applications with the help of the app permissions, and also the various methods describe in this paper.**

Keywords---Mobile, Android, Permission Analysis, Malware, Machine Learning, Static Analysis

I. INTRODUCTION

Smartphones have become a necessary part of our daily lives in recent years since they are involved in keeping in touch with friends and family, doing business, accessing the internet and other activities. Andy Rubin, Google's director of mobile platforms, has commented: "There should be nothing that users can access on their desktop that they can't access on their cell phone"[1]. So smartphone sales are continuously on the rise and more and more people are becoming dependent on these devices. In the current era, 90% of peoples are using smartphones which are based on platforms Android, IOS, Blackberry, Windows, etc. And most of the people are using the Android-based platform mobile.

Android applications are made by smartphones more "smart". Google, Apple, and other third-party providers use "app stores" for convenient online sources for free and paid apps to be easily downloaded and installed. The official Google app store is Google Play. According to Hypponen and Tuominen (2017) of the cybersecurity firm F-Secure, there have been over 19 million malware programs developed specifically targeting Android which accounts for 99% of all malware targeting mobile devices in general. Some features of the Android Operating system given in the following[2]:-

Apps (Applications)

Apps making our smartphone more than just a phone. Android OS is defined as apps in terms of components that are its key building blocks. There are four app components available in the android OS like, Activities, Services, Broadcast Receivers, and Content Providers. Activity is the entry point for interacting with the user. Service is used for keeping an application running in the background to perform some long-running operation. Broadcast Receiver is listening to the system generated events, or conversely enables the system to deliver events to the app directly outside of normal user flow. Content Provider manages a shared set of app data so that it can be stored in the file system, on the web, in an SQLite database or storage location.

Permissions

Permissions are an important part of the Android Operating system. The purpose of permission is to protect the privacy of the user. Applications are required to request permission to access sensitive data of the user. Android categorizes permissions into four categories which are given in the following:-

Normal Permissions that have a minimum risk on the user, system or the device and granted by default at the install time.

Dangerous Permissions that are evaluating high risk because of their capability of accessing the private data and important sensors of the device.

Signature Permissions are granted only if the requesting application is signed by the same certificate as the app that defined the permission.

Special Permissions are system-level and in general unavailable, to apps although there are methods for acquiring.

Intents

The other important thing about the Android Operating System is intents. An intent is a messaging component used to request an action from another app component. There are two types of intents which is given in the following:-

An explicit intent is to specify precisely which app will satisfy the intent. This is typically used to start a component within the same app such as starting a new activity in response to a user action.

Implicit intent does not name a specific component but rather declares an action to perform for which a component from another app can manage.

Android security is complex and we evaluate an application development environment that is susceptible to malware attacks. Mobile malware is a malicious software code/program and the main intention of this malicious software is to damage mobile devices. The main purpose of the malicious software is to steal confidential data or to obtain root privileges. The whole study regarding the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 04, April-2020

malicious android app shows that the effect of the malware is failing step by step exceptionally in the banking and financial section. That's why it is important to study different types of malware, their impact, and their detection techniques.

II. LITERATURE REVIEW

There are many existing relevant approaches are available in the market which is detected the malicious applications. But these approaches provide a little bit of flexibility to query which is based on a set of suspicious permission. For detecting android malicious application APP PERMISSION is the most important thing. Many preventive tools are available in the market but in the current market for malware security is before installing the app user should able to identify whether the applications are malicious or not. Hence there are several proposed methods available for permission-based mobile malware detection systems using Machine Learning.

Basic Of Android Operating System[3]: The main objective of this paper is to introduce the Android Operating system. Android is day by day updating since its release. These updates mainly focusing on fixing bugs as well as adding new features to provide a more user-friendly environment. Every new version of the Android operating system is developed under a code name based on the dessert item, but it applies only up to android version 9. In this paper android operating system and it's version's history are described.

Secure Sockets Layer (SSL):- The SSL and its successor, Transport Layer Security, are cryptographic protocols that were introduced to protect network communication. To establish a secure connection, a client must securely gain access to the public key of the server.

Android Security :- Android kernel is to build security measures n the OS is sandboxed and preventing malicious processes from crossing between the applications.

Service :- A service is one type of code, which is long-lived and runs without the UI design. StartService() is to run the service in the background.

Some features of the Android Operating System are also described in this paper like Storage, Connectivity, Messaging, Multiple language support, Web browser, Java Support, Multi-touch, Bluetooth, Tethering, Screen capture, and Video Calling.

Android Data Storage Security[4]: Based on the "Mobile Security Project" under "The Open Web Application Security Project (OWASP)" the insecure data storage is the biggest issue in smartphones since sensitive information can be disclosed if it is not protected carefully. The main aim of this paper is about the insecure data storage on Android smartphones which is expanding the coverage of security threats and solutions. The solution method of this objective is CleanOS, TinMan, Sentry.

CleanOS :-

CleanOS is the prototype of an Android-based operating system. In this, the sensitive data in RAM are identifying and internal storage which is unused for a specific amount of time then encrypt them and then store the encrypted keys in the cloud. This does not protect the data which is in use.

TinMan :- TinMan is the prototype system which is used as an offloading mechanism. It separates the credentials access from the rest of the functionalities of the app. TinMan provides a trusted node for storing those credentials. Focuses on confidential data like password, bank account, social security number and credit card number which is known as the confidential record. The main aim of this method is to avoid storing sensitive data on the device, so whenever the device is lost or stolen, there is nothing to lose.

Sentry :-

Sentry method is encrypted memory pages of the sensitive application. It encrypts the sensitive application when the screen of the device is locked and decrypt when the screen of the device is unlocked. Android storage model options and security also shown in this paper. There is a set of identified threats on Android data storage with the solutions. Also discussed the Biometric cryptosystem substitutes password-based encryption method. It can be used for secure data against software attacks since data is encrypted.

Significant Permission Identification for Machine Learning[5]: The main objective of this paper is to identify the weather the application is malicious or not. So for this, this paper is introduced the SIGPID method for malware detection systems based on the permission usage analysis. In this method, the author develops the 3-levels of pruning by mining the permission data to identify the most significant permission that can be effective in distinguishing between malicious and benign apps. As an output or result, researchers use machine learning and mining techniques to detect Android malware based on permission usage.

In the SIGPID method, first, it extracts significant permission from apps and uses the extracted information to effectively detect the malware using supervised learning algorithms.

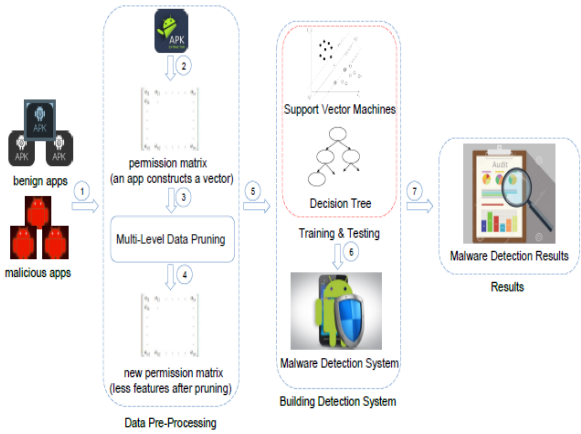

Fig. 1. Architectural Overview of SigPID

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 04, April-2020

The main three major components that this system consists, which is given the following:-

- Permission ranking with the negative rate
- Support based permission ranking
- Permission mining with association rules

This approach referred to as Permission Ranking with Negative Rate or PRNR, which provides a concise ranking and comprehensible result. This approach work on the two matrices, M and B. In this M stands to list of permissions used by the malware samples and B stands to list of permission used by the benign apps. In this Mij represent whether the jth permission is requested by the ith malware sample, while '1' indicates the YES, and '0' indicates the NO. Bij represents whether the jth permission is requested by the ith benign app sample.

In this paper, they compare the results between malware detection rate using all identified 135 permissions and malware detection using MLDP for each supervised machine learning algorithm. SIGPID has been designed to extract only significant permissions through a systematic, 3-level pruning approach. SIGPID is highly effective when compared to the state-of-the-art malware detection approaches as well as existing virus scanners. It can detect 93.62% of malware in the data set, and 91.4% unknown or new malware.

Permission Analysis for Android Malware Detection[6]:
The main objective of this paper is to detect the android malware application on the bases of permission. The already existing relevant approaches which identify the malicious applications suffer from the performance problems where the occurrence of false-negative remain high. So for this problem, this paper introduced the Latent Semantic Indexing (LSI) method for identifying malware applications. In this paper, the author applied the two-phase of analysis like Static and Dynamic. LSI is the most known information retrieval technique where a set of words is used to identify the most relevant set of documents. This technique computing a matrix where the rows are set of words, and columns are a set of documents. After this matrix is reduced for finding the most important set of documents using singular value decomposition.
In this paper, the author examines the permission lists present in the XML files after the decompiling of the android application's apk using appropriate tools.
To reduce the false-positive warning, the author confirms the maliciousness by testing the application within a sandbox. If in the sandbox environment, the application shows the expected behaviors matching with the list of the permissions, then declared the application as anomalous.
So Android applications by identifying the most relevant category of the permissions to match from and then confirming behaviors in an emulator environment. The main relevant category is identified using the Latent Semantic Index (LSI) analysis. This method has the potential to discover new malicious android applications that are coming in the market.

The future work of this paper is to evaluate more applications and query types and apply the approach to address other security vulnerabilities.

III. COMPARISON OF METHODS

Sr-No	METHOD	PROS	CONS
I.	CleanOS[4]	Encrypt sensitive data and save the keys in the cloud.	Do not protect data in use. Vulnerable to network attack.
II.	TinMan[4]	Separate confidential data and save them in a trusted node.	Hard to identify confidential data that reside in many places. App's performance degradation.
III.	Sentry[4]	Secure the encryption keys by preventing saving them in the RAM.	Lead to lower performance.
IV.	Significant Permission Identification[5]	Achieve high malware detection accuracy and efficiency while analyzing the minimal number of permissions.	Designed to extract only significant permissions through a systematic.
V.	Latent Semantic Indexing(LSI)-based Permission Analysis[6]	The approach has the potential to discover new anomalous applications	It's not divided the application into the categories. Users can not use that app without harm their data.

IV. CONCLUSION

Mobile application security is complicated; it is not just the code running on the devices, there are innumerable other factors like the device platform, web-service, and cloud-based 3rd party services, etc., that is perform a most important role in mobile application security. In the mobile application the main important thing is permission, and due to the permission attackers try to get the user's sensitive data and information. The literature exposes the basics of the Android Operating System and provides solutions to the android malware applications. In this paper, we have shown that it is possible to reduce the number of permissions to be analyzed for mobile malware detection while maintaining high effectiveness and accuracy. In this paper various machine learning approaches described for detecting malicious Android applications.

V. REFERENCES

[1] MOBILITY 2015 - The Fifth International Conference on Mobile Services, Resources, and Users http://www.researchgate.net/publication/278968819.
[2] Fred Guyton, "A Survey of Android Security threats and machine learning techniques used for detection".
[3] Kirthika.B, Prabhu.S and Visalakshi.S. “ANDROID OPERATING SYSTEM: A REVIEW “, International Journal of Trend in Research and Development, Volume 2(5), ISSN 2394-9333, Sep - Oct 2015.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 04, April-2020

[4] Altuwaijri, H., Ghouzali, S. “Android data storage security: A review”, Journal of King Saud University – Computer and Information Sciences (2018).
[5] Jin Liy, Lichao Sunk, Qiben Yanz, Zhiqiang Liz, Witawas Srisa-anz and Heng Yexy. Significant Permission identification for Machine Learning Based Android Malware Detection. TII.2017.2789219, IEEE.
[6] Hossain Shahriar and Mahbubul Islam, Victor Clincy. Android Malware Detection Using Permission Analysis ,2017, IEEE.
[7] Muneer Ahmad Dar & Javed Parvez, “Evaluating Smartphone Application Security: A Case Study on Android”, Global Journal of Computer Science and Technology (E) Volume XIII, Year 2013.
[8] Cassandra Beyer, “Mobile Security: A Literature Review”, International Journal of Computer Applications, Volume 97-No.8, July 2014.
[9] Daojing HE, Sammy Chan, and Mohsen Guizani,”Mobile Application Security: Malware Threats and Defenses”, IEEE Wireless Communications, February 2015.
[10] Sardasht M. Mahmood, Bakhtiar M. Amen, Rebwar M. Nabi, “Mobile Application Security Platforms Survey”, International Journal of Computer Applications(0975-8887),Volume 133-No.2, January 2016.
[11] Zhou Ziqiang, Sun Changhua, Lu Jiazhong, Lv fengmao,”Research and Implementation of Mobile Application Security Detection Combining Static and Dynamic”, IEEE 2018 10th International Conference on Measuring technology and Mechatronics Automation.