IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11655

Android Risk Privacy Risk Assessment Tool on Android

Kandala Prakash[1], G. Rajesh[2], D. Anand Joseph Daniel [3], M. Maheswari[4]

Student, B.E. Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[1,2]

Assistant Professor, CSE, Anand Institute of Higher Technology, Chennai, India[3]

Assistant Professor, CSE, Anand Institute of Higher Technology, Chennai, India[4]

Abstract: On Android, every application operates during a basic sandbox and is prevented from accessing additional services that need users' consent. These services can only be accessed if users allow the appliance to use them. Granting of permission is static and may only be done at the time of the installation of the application. Android security model leaves most of the labor for security-related approaches to the user. LibreAV is an endeavor to detect malware on Android devices employing a machine learning approach that is powered by the Tensor flow. We use a two-layer neural network trained with a set of features. The neural network is tuned in such the simplest way that it performs efficiently on mobile devices where computational resources are limited. Testes show that LibreAV performs efficiently and effectively even on low-end mobile devices. With LibreAV, you'll be able to scan all the installed apps on your device in an exceedingly matter of seconds. It also encompasses a real-time scan feature that alerts you whenever an app is installed or updated. Neural networks and SHA scan the applications and predict potential malicious behavior using state-of-the-art Machine Learning algorithms.

I. INTRODUCTION

Android users face many threats and risks. Since modern mobile devices are almost all the time exposed to the internet and other types of mobile networks, they are more exposed to attacks. From the open Wi-Fi networks that can be spoofed to the Trojan malware applications on the app stores, threats are everywhere around. Many of the attacks are successful because users are not aware of the risks and threats. These attacks may lead to identity theft, money theft, or losing privacy or the devices may start acting as part of the botnet network. In order to prevent attacks on the users, this project aims to develop a set of guidelines and applications that will ensure that users are using their devices in a secure manner. The project is and always will remain open for everyone to participate and all project deliverables will be free and open source.

1.1 OBJECTIVE

To detect the threats and risks. The main objective of this system, A user will use internet and other types of mobile networks, they are more exposed to the attacks. The mobile application need some permission and default ask to user which harm to device. In order to prevent attacks on the users .Creating set of Guidelines and application that will ensure that user knows how application are secured.

1.2 SCOPE

SeraphimDroid takes a heuristic and machine learning approach to find out the potentially malicious or harmful application installed on the user's phone. These are based on the permissions this application uses, but besides that, it provides some other security and privacy features as well.

II. ANALYSIS

2.1 SYSTEM ANALYSIS

System Analysis is a combined process dissection the system responsibilities that are based on problem domain characteristics and user requirement.

2.1.1 Problem Definition

Mobile devices become popular present world. Since they offer almost the same applications on android mobile. Android-based smartphone users can download and install many applications. But with this application may cause threats and risks. Because some applications were not certified. They have some malware or without knowing the user it takes permission from the users and it may steal the user's privacy.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11655

2.1.2 Existing System

The mistakes can happen knowingly or unknowingly from the developers likewise as users. These mistakes may result in threats arising to Android OS and its applications. it's been identified that users are to blame for most security issues. Some common mistakes done by the users will result in serious threats in an Android application. At the time of putting in Android applications, users are asked to permit some permissions. However, all the users might not understand the aim of every permission. they permit permission to run the application without considering the severity of it. Fraudulent applications might steal data and perform unintended tasks after getting the specified permissions. it's possible to arise threats to the Android systems thanks to the mistakes performed by the app developers at the time of developing applications. within the publishing stage of the Android apps, Google Play will have only limited control over the code vulnerabilities within the applications. Sometimes developers are specifying unwanted permissions within the Android manifest file mistakenly, which inspires the user to grant the permissions if the permissions were categorized as not simple permissions.

2.1.3 Proposed system

Malware attacks are the foremost common case that may be identified as a threat to Android. There are various definitions for malware given by many researchers betting on the harm they cause. the final word meaning of malware is any malicious application with a bit of malicious code that has an evil intent to get unauthorized access and to perform neither legal nor ethical activities while violating the three main principles in security: confidentiality, integrity, and availability. Malware associated with smart devices are often classified into three perspectives as attack goals and behavior, distribution and infection routes, and privilege acquisition modes. it's a requirement to detect malicious inter-app communication and app permissions for app collusion detection. With LibreAV, you'll scan all the installed apps on your device in a very matter of seconds. It also contains a real-time scan feature that alerts you whenever an app is installed or updated. Neural networks and SHA scan the applications and predict potential malicious behavior employing a state-of-the-art Machine Learning algorithm.

III. SYSTEM DESIGN

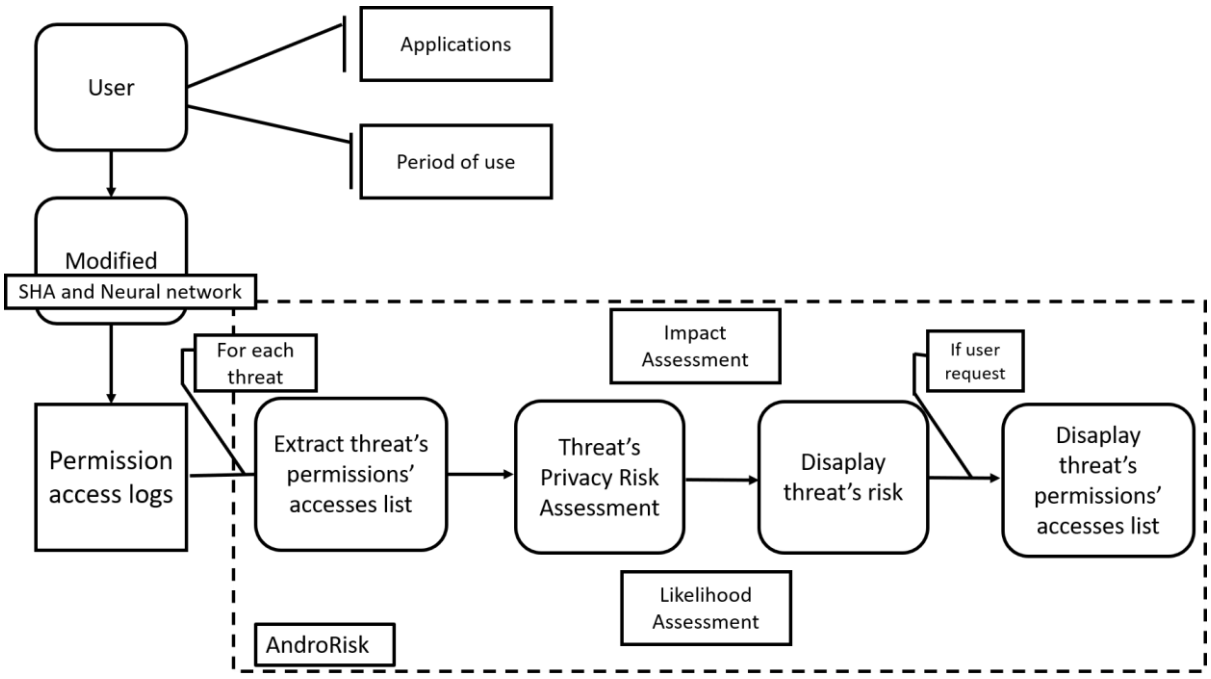

Figure 1.Overall Architecture Design

IV. MODULES

SHA takes a heuristic and machine learning approach to find out the potentially malicious or harmful application installed on the user's phone. These are based on the permissions this application uses, but besides that, it provides some other security and privacy features as well. All the features that Neural Network provides are:

1. Permission Scanner

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.11655

2. Settings Checker
3. Android Permission Check
4. Privacy Policy Database
5. Application Uninstaller

All these features are helpful to the user and help him prevent his phone from harmful applications, data theft, and unwanted money loss to premium services and device theft. These services are explained briefly.

4.1 PERMISSION SCANNER :

The scanner will go through all the installed applications on the user's device and will scan all the permissions each application uses. Then it will fetch the details about each permission and show the application as red (harmful) or green (safe). The Machine Learning algorithm will predict the malicious behavior of the application based on the respective permissions. The labels predicted are:

1. Green: The application is unlikely to show malicious behavior
2. Red: The application is likely to harm the user's device, data, or both Based on the Flags allotted to the Application, you can uninstall the Application.

4.2 SETTINGS CHECKER:

The Settings Checker scans the user's device for vulnerable settings and informs him about the potential vulnerabilities that can arise from these. It also gives him a one-click shortcut to go directly to the respective settings page, so he can change it directly. Neural Network by default performs a daily scan of the settings and notifies the user via a notification. The user can choose to perform a weekly, fortnight, or monthly scan by selecting the respective option in the settings.

4.3 MALWARE APPS ANALYZER:

In today's digital world most anti-malware tools are signature-based which is ineffective to detect advanced unknown malware viz. metamorphic malware. In this paper, we study the frequency of opcode occurrence to detect unknown malware by using the machine learning technique. We also studied multiple classifiers available in App GUI-based machine learning tools and found that two of them (Neural Network and SHA) detect the malware with almost 100% accuracy

4.4 ANDROID PERMISSION CHECKER

A user who wishes to put in and use any third party app doesn't understand the importance and meaning of the permissions requested by an application, and thereby simply grants all the permissions as a results of which harmful apps also get installed and perform their malicious activity behind the scene.

4.5 PRIVACY POLICY DATABASE

We presented a novel approach to the analysis of privacy policies in the context of Android applications. The tool we implemented greatly eases the process of understanding the privacy implications of installing third-party apps and it has already been proven able to highlight worrisome instances of applications.

4.6 APPLICATION UNINSTALLER

This could be considered as more of a privacy feature as user will be able to prevent access to certain applications like gallery, people, etc. to others who might access his phone. This will secure others access to user's content and hence is essentially a privacy enhancement. User will have the power to uninstall any application and uninstall it. Whenever a locked application is started a password prompt is shown, on entering the correct password only the uninstall application can be accessed else the application will be terminated.

V. RESULTS AND DISCUSSION

Seraphim Droid aims **to supply a close** explanation and documentation on the permission that the android application uses. **a number of** the permission could cause harm to users' money and data, SeraphimDroid scans the applications and predicts potential malicious behavior using state of an art Machine Learning algorithm. SeraphimDroid **will** evolve **to produce** a system for blocking access to premium services without the user's permission.

• An unaware user might keep his device on settings **that may** open up security vulnerabilities, Seraphimdroid's "Settings Check" feature scans vulnerable security settings and notifies user of the potential harm **and therefore the** optimal setting that he should switch to.

• Although the android architecture provides a **over** a solid platform **that's** secure and at **the identical** time robust there are **some** bits that **don't seem to be** included **within the** default android systems. Android **encompasses a** layered

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.11655

architecture **and every** process runs separately from **each other** in its own sandbox but this doesn't **make sure the** protection of the device from all the privacy attacks and clearly not from device theft. SeraphimDroid was developed keeping in mind only the looped aspect of the Android security architecture and was focused on securing users from losing money and giving documentation of permissions, but **it's** evolved into an anti-theft and privacy-protecting application.

• Another such useful enhancement is Geo-Fencing. An anti-theft advancement for **the appliance**. It allows the user **to make** virtual fencing for the user's device and if the device moves out of the fencing, **it's** assumed that the device is being stolen and it starts performing operations **like** locking the device and wiping data, ringing siren, etc. **to safeguard** itself. Of course, the user could control which operation to enable and **to not** enable. This looks quite complete but **just in case** the user forgets to enable fencing he still **has got to** power to perform this operation which **may be** triggered **employing a** special SMS. The SMS will contain a **code** on receiving which the phone will perform these features and moreover it could send you its current location coordinates

VI. CONCLUSION

Although not 100% complete, we feel we successfully:

• Exhibited the feasibility of a user approach for privacy risk assessment.
• Suggestion of a method that takes in consideration diverse source of inputs
• Created a platform from which future work can be accomplished.
• All source code will be provided with our final report submission.

REFERENCES

[1]. Ali Reza Galib, Nafize Ishtiaque Hossain, Raihan Bin Mofidul, 19 December 2019, A Vision Based Three-Layer Access Management System withIoT Integration.
[2]. Brajendra Panda, Jonathan White, 8-11 June 2009, Implementing PII honey tokens to mitigate against the threat of malicious insiders.
[3]. Gilchan Park, Julia Rayz, 7-10 Oct. 2018, Ontological Detection of Phishing Emails.
[4]. Guanyu Yan , Qinlong Huang, 03 September 2021, Privacy-Preserving Traceable Attribute-Based Keyword..Search in Multi-Authority Medical Cloud.
[5]. Jiawei Zhao, Rahat Masood, Suranga Seneviratne, 04 June 2021, A Review of Computer Vision Methods in Network Security.

