International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

ROOT SECURITY FIREWALL

G. Mathan[1], M.S Mohamed Rasith[2], R. Praveen Kumar[3], S. Sathish Kumar[4]

[1,2,3]UG Student, Dept of CSE, SNS College of Technology, Coimbatore.
[4] Associate Professor, Dept of CSE, SNS College of Technology, Coimbatore.

ABSTRACT- *In Mobile environment, Android-Security is becoming a notable feature of today's Android Phones and tablets where users can download unknown apps, spyware's and connect their Android device to unknown networks when its roaming and using public networks without knowing the risk. This project proposes and entrust an enhanced monitored security model and architecture for Android platform. In recent years, the amount of malicious(spyware) mobile application and malware targeting android based smartphones and portable devices has increase rapidly and security decreased respectively. Thus, the security for the android mobile is most needed. Root Security Firewall (RS Firewall) can grand or revoke the network permissions and monitor other applications and show the front-end that application access the android network permission. This RS firewall can monitor other application activity mainly their android permission access (network) and display them to user with check box. RS Firewall have the list of applications that's installed in the Android Mobile. RS Firewall have the network permission access and it can grant or revoke network permission to other applications. Thus, RS Firewall made the Android device network transparent as the checklist to the user then the user can grant or revoke the network permission to all applications in android by this approach Android can access the network in control manner. Here we improve the Security of the Android device by network monitor firewall.*

***Key Words*: Firewall, Android Security, Cyber security, Privacy and Android Application.**

1. INTRODUCTION

The RS Firewall app is an Android Firewall Application but had some extra secure functionality for Networks. Before presenting more features concerning RS Firewall, we will prevent some of anti-malware and spyware strategies, which we believe are important to ensure security in our Application. Note that these strategies are general strategies, which are used on various clients like Microsoft, Linux, and Mac OS. Some of the anti-malware and anti-spyware Process require the user interaction to decide what to do with malicious applications either which are not clearly safe or not clearly malware. Nowadays, anyone can develop Android applications with Android application development tools and without having strong programming skills. So, the market price of developing Android applications is very low. Most of the companies and developers do not have proper security skills, to create a proper secured Android application.

Therefore, the developers sometimes do not consider all security issues and that's leads to insecure, they are simply not skilled enough to be aware of all vulnerabilities and risks. However, the user is often not in the best position to decide. We therefore propose that the user choose a security policy. There could be two different security policies, which the user could use One anti-malware strategy is to grant permission to all Unknown applications. Another anti-malware strategy is to deny permission to all Unknown applications.

The problem with all these strategies is that all are far too general. Our solution's main component is as mentioned, an Extreme Network controlled Environment for Android Mobile. The network is most important in Android smart devices and it is the key for the data theft the malicious applications use the network to be spying the device and transfer the data through network and some hacking also done by network like honeypot. The second component is, also as mentioned, the RS Firewall Application use the afwall+ Server maintaining a iptables to provide secure network access to the applications, including their status and other statistics. A simplified version of the RS Firewall Application. By the Access of Super User, we can grand or revoke permissions to the installed applications. The android has the permission control feature by that we can grand the permission for that mode of safe network or revoke the permission for the mode of unknown network.

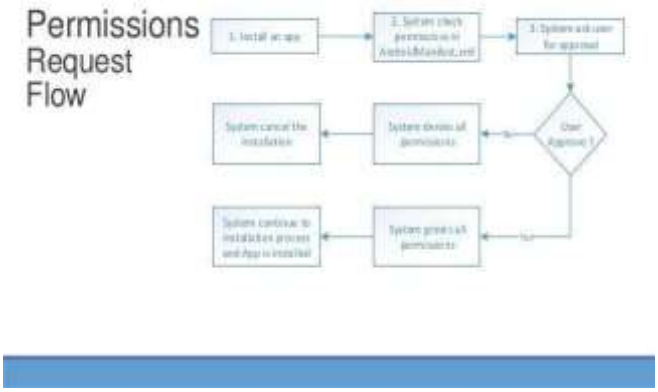

Fig -1: Permissions Request flow

2. LITERATURE SURVEY

1) P. D. Meshram, Department of Information Technology, "SGGSIE&T Nanded" and Dr. R.C. Thool, Department of Information Technology, "SGGSIE&T Nanded" in Conference December 2014, DOI: 10.1109/GCWCN.2014.7030873. [1]

The amount of malicious mobile application targeting Android based smartphones has increase rapidly. In addition, these malicious apps can download modules from servers which are run by malicious users, meaning that unexpected events can be activated inside of smartphones [3]. Therefore, the attacker can control and get personal information and data stored inside of smartphone illegally. Smartphones are not just phones but also portable computers, providing diverse services needed in life including calls, texts, emails, GPS, camera, Wi-Fi and Bluetooth apps. These apps keep and manage diverse intrinsic data as well as sensitive private information such as address books. Smartphones enable swift and easy data exchange via 3G, 4G and Wi-Fi. Thus, personal information stored on Smartphones is prone to leakage.

2) Caner Kilinc, Todd Booth, and Karl Andersson Pervasive and Mobile Computing Laboratory, "Luleå University of Technology" in 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. [9]

- WallDroid: Cloud Assisted Virtualized Application Specific Firewalls for the Android OS.
- Cloud keeping track of millions of applications and their reputation (good, bad, or unknown) and comparing traffic flows of applications with a list of known malicious IP servers.

3. PROPOSED SYSTEM

Most of the people are using smart phone. So, Security for the Smart Phone is need most. Thus, we Proposed the system "ROOT SECURITY FIREWALL" (RS Firewall). Which can monitor other application activity mainly their android Network permission access and display them to user in the Application UI as simple check box. The user could decide the application is malware or not. The internet is main thing in hacking, so RS Firewall can grant and revoke network access to all applications in Rooted Android Platform. RS Firewall have the list of applications that's installed in the Android Mobile. RS Firewall have the network permission access and it can grant or revoke network permission to other applications. Thus, RS Firewall made the Android device network transparent as check list to the user then the user can grant or revoke the network permission to all applications in android by this approach Android can access the network in control manner. Here we improve the Security of the Android device by network monitor firewall.

RS Firewall have both white list approach and the blacklist approach by this it's become handy in many situations. If we need only few application in the network we connected means we can use white list approach that only allow selected application to access the network else we need to block only some application means can use blacklist approach that restrict selected application from access the network and their network permission access and it can grand or revoke network permission to that selected applications. RS Firewall have the button on/off which is used to access the permission. RS Firewall can show the application access history(log) on Android Security permissions. By knowing the application Permission history user can block harmful permissions.

Fig -2: Proposed Application

4. MODULE DESCRIPTION

4.1 Network Module:

- List of Application

RS Firewall have the list of applications that's installed in the Android Mobile.

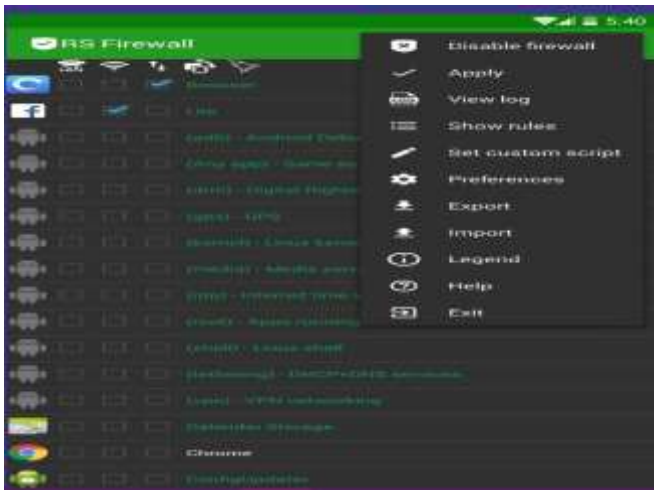

Fig - 3: List of applications and options

- Network Permission

RS Firewall have the network permission access and it can grant or revoke network permission to other applications.

- Button

RS Firewall have the button on/off which is used to access the permission.

4.2 Permission Module:

- List of Application

RS Firewall have the list of application which in order of the installed time or its permissions based

- Network Types

RS Firewall can show the application network access type on Android Security permissions like wifi, mobile data, lan. etc..

- Block Permissions

By knowing the application Permission history user can block harmful network access permissions.

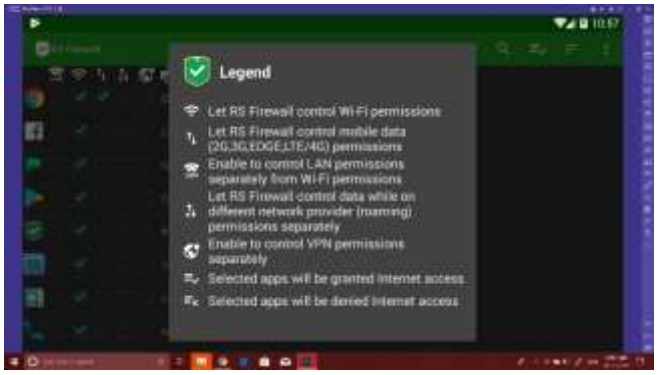

Fig - 4: Symbols used

5. CONCLUSION

In this modern era, people have been using Smart devices particularly Android devices. There is no security in Android compare to the apple platform. who do not have a knowledge about androids their devices can easily hacked. The important factor of hacking is transmission medium, here it is networks. Hence RS Firewall ensures the security of the android platform that they control all other application networks Permissions by the Authority of Super User. It has simple user interface like checkbox So it is User Friendly.

REFERENCE

1. A survey paper on vulnerabilities in Android OS and Security of Android Devices at: https://www.researchgate.net/publication/280096665
2. Afwall+ - https://apkpure.com/afwall-android-firewall/dev.ukanth.ufirewall.
3. Android API Guide - Permission, http://developer.android.com guide/topics/manifest/permissionelement.html.
4. Android Permission, https://android.googlesource.com/platform /frameworks /base/+/master/core/res/AndroidManifest.xml
5. Android Proguard, http://developer.android.com/tools/help/ proguard.html.
6. ContentProvider, http://developer.android.com/intl/ko/reference/android /content/ContentProvider.html.
7. Dalvik, http://ko.wikipedia.org/wiki/%EB%8B%AC%EB%B9%85_(%EC%86%8C%ED%94%84%ED%8A%B8%EC%9B%A8%EC %96%B4.
8. Smali, http://code.google.com/p/smali/.
9. WallDroid: Cloud Assisted Virtualized Application Specific Firewalls for the Android OS -2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.