VPN Service in Android for Monitoring Network access by Applications

Amit Kumar Rai

Research and Development, Syscom Corporation Limited

Abstract- This paper describes the requirement of Firewall Service in the Android Architecture for restricting the access of applications and Services from using shared resources and network access.

Index Terms- Firewall, Android, Services, Access

I. Introduction

Android platform is an open source platform. Open source platform provides freedom to developers for creating many useful applications and services. But there are also problems with Open source platform. As the code and libraries are open source therefore everyone knows how to exploit them to perform malicious activities. Talking about the Android Operating System, it is the most famous Open source application created till date.

This has also made it more prone to issues which not only affect the software but also can affect the performance of the device on which it is running. Therefore, It is very important for Android developers to save Android devices against hackers searching to destroy the data or to use that data for deceitful activities. Although it has inbuilt security system but it is still vulnerable to unauthorized access. Applications when installed on it require different kind of permission which sometimes is beyond understanding of a normal user. This allows malicious programmers to program application that can access system resources and user data also. Also, there are applications installed on the system which are not malicious but consumes to much system resources for example battery of device.

These applications are granted permissions like access to internet when installed on the system, so they keep on accessing the network from backed even when user does not require to access. Even when the application is removed from the processes, it starts after some time and again start to consume system resources. For example, Facebook application requires to access internet services to get updates from the server and in this process it will keep on pinging the internet service which in result will consume the GPRS data, RAM of device as well as Battery also.

Firewall in Windows in a service which imposes this restriction on access of resources both internally and externally. It imposes a shared access policy with connection sharing service to restrict the applications and services as shown in following diagram:

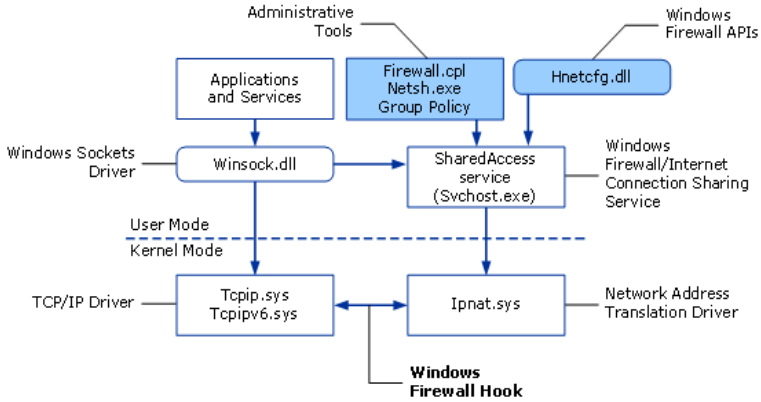


Figure 1: Windows Firewall Service

Firewall applications works like a filter mechanism [3] between the system (your computer) or network and the internet. You have the privilege to program what you want you want to allow in and what you want to allow out of our system or network. There are many different firewalls that can be used on Windows environment to filter out information, and some can even be used in combination. These methods work at different layers of a network, which determines how specific the filtering options can be.

But this kind of facility is not available in Android Operating System. It does not come with any built in firewall mechanism. Currently there are two kinds of measures available to restrict these applications and services from consuming the resources. One of these measures is restricting the services manually. This requires rooting the android OS. But the rooting process is not an easy process and also requires a level of expertise to do so. Rooting the Android OS itself is dangerous because of two reasons:

1. It will void the warranty of the phone and
2. It can make the OS as well as Phone Brick. And a Bricked phone is beyond repair.

Second measure is to use already existing applications. But these applications also require rooting of the Operating System. Another is to use NoRoot Android Firewall Application. This application provides firewall like functionality and user can select which kind of service it want to grant access. And whenever an application or service will require access to internet resources it will give notification to user and will ask if he/she want to allow the application/service the access or deny it. Using this application also has pitfalls of its own. First this application is required to provide VPN access. This means allowing the

application to monitor the network used by the user which for security reasons is not a good thing because of following reasons:

1. According to Android Developer website developer.android.com, *"Letting any application create a VPN connection leads to huge security concerns. A VPN application can easily break the network. Besides, two of them may conflict with each other. The system takes several actions to address these issues.*[1]"

Also there can only be one VPN connection running at the same time. The existing interface is deactivated when a new one is created.

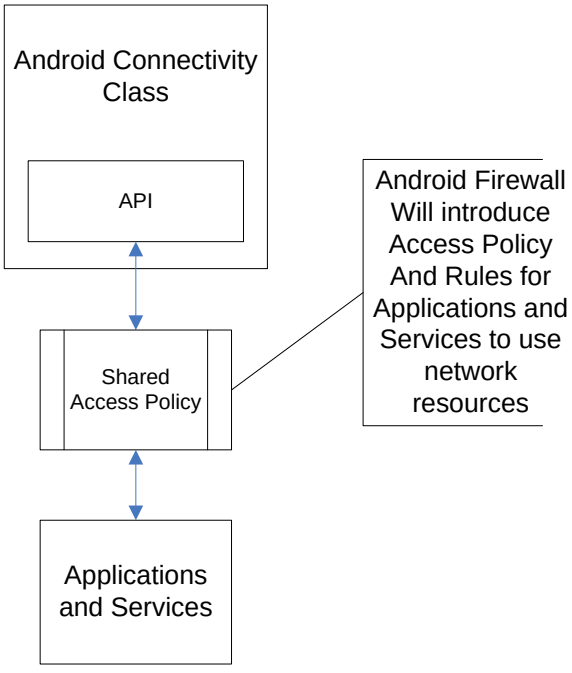
2. Secondly this application itself uses system resources and also requires granting permissions on the device. We don't know what kind of data it is reading from the device and sending to the server from backend.

Proposed modification: The proposal to overcome these pitfalls and restrict the services is to introduce a Firewall system in the android OS itself. The Inbuilt Firewall will be used to grant access to the services and applications and will include all features which the third party applications claims to provide and no rooting will be required for this also.

II. Implementation

Android's Connectivity Manager Class provides answers to the queries about the state of network connectivity and also notifies applications when network connectivity changes.

Android Firewall will introduce a shared access policy in the system to provide access to the resources required by the applications and services. This will be done by controlling the access to the Connectivity class.



This class performs following activities:

1. Monitoring network connections
2. Sending broadcast intents when network connectivity changes
3. Provide an API that allows applications to query the coarse-grained or fine-grained state of the available networks
4. Provide an API that allows applications to request and select networks for their data traffic.

For implementing the firewall service in simplest manner is to modify the already available VPN service of Android. Android has integrated user level support for VPN services for PPTP and L2TP VPNs.

How does a VPN works:

When you connect a smart phone to a VPN network, the device will behave as if it's on the same local network as the VPN to which it is connected [2]. All the network traffic will be sent over a secure connection to the VPN. Since the device is acting like it is on the same network, it will allow you to access the network resources and you can use the Internet as if you were present at the VPN's location.

Conceptually, VPN service can be integrated as an inbuilt application or service that will come with android OS which will route all data through it. This feature can be implemented as follows:

1. Android Monitor service can be created in Android which can be activated deactivated by user just like any other inbuilt service.

2. When this service will be activated, it will create a VPN network and all network connection will be routed through this service only.

3. This service will then create list of an all applications that require internet access (Since all application that require internet access ask for permission during installation, this service will keep on check for applications that are asking internet permission while installation).

4. Whenever any application will try to access network, this service will block the access if configured by the user or will provide notification to user to grant or deny the access.

5. User can create service rules for when to be active or when to start monitoring network for example, when consumption of user data increases a certain limit(as calculated in data usage feature of the Android service.

III. CONCLUSION

Using already available services of Android, Network access can be controlled and monitored for different applications. This will provide an Android user control over the services and application in the system and will provide a better user experience.

REFERENCES

[1] VPN Service Implementation in Android, developer.android.com
[2] How VPN works, http://computer.howstuffworks.com/vpn.htm
[3] HOW Windows Firewall Works, https://technet.microsoft.com/en-us/library/cc755604%28v=ws.10%29.aspx

Authors

First Author – Amit Kumar Rai, rai.amit@hotmail.com