OWASP Seraphimdroid Guide

By Nikola Milosevic, Furquan Ahmed, Kartik Kohli & Aditya Dua

Project 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 the 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. They may act naive and expose themselves to the attacks even more. These attacks may lead to the identity theft, money theft, losing privacy or they 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 application that will ensure that users are using their devices in a secure manner. Project is and always will remain open for everyone to participate and all project deliverables will be free and open source.

Mission of OWASP Seraphimdroid project is to create, as a community, an open platform for education and protection of Android users against privacy and security threats.

On Android, every application operates in a basic sandbox and is prevented from accessing additional services that require users consent. These services can only be accessed if users allows the application to use them. Granting of permission is static and can only be done at the time of the installation of the application. Android security model leaves most of the hard work for security related approach to the user. SeraphimDroid aims to provide detailed explanation and documentation on the permission that android application uses. Some of the permission could cause harm to user's money and data, SeraphimDroid scans the applications and predicts potential malicious behaviour using state of the art Machine Learning algorithm. SeraphimDroid will also evolve to provide a system for blocking access to premium services without user's permission.

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

Although the android architecture provides a more than solid platform which is secure and at the same time robust but there are few bits that are not included in the default android systems. Android has a layered architecture and the each process runs separately from one another in its own sandbox but this doesn't ensure 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 user from losing money and giving a documentation of permissions, but it has been evolved to an anti-theft and privacy protecting application.

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

Overview

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 these application uses, but besides that it provides some other security and privacy features as well. All the features that SeraphimDroid provides are:

1. Permission Scanner
2. Settings Checker
3. Call / USSD blocker
4. SMS Interceptor
5. Application Locker
6. Service Locker
7. Geo-Fencing
8. Remote Lock / Wipe
9. Knowledge Base

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

Permission Scanner

The scanner will go through all the installed application 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 behaviour of the application based on the respective permissions. The labels predicted are:

1. Green: The application is unlikely to show malicious behaviour
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

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.

SeraphimDroid 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.

Call / USSD Blocker

The blocker is built in the application to block outgoing numbers which is not saved in the user contact list but now it has been evolved to provide the blocking control to user. The user could choose to block calls as he wants from the setting. A blacklist is also implemented which will allow user to block only certain numbers on his will.

On the other hand the USSD blocker is something kept out of the reach of user but blocks all the dangerous USSD that could be entered. USSDs includes code to factory reset, delete user’s data or lock the phone. The USSD blocker prevent these harmful codes from being executed.

SMS Interceptor

SMS Interceptor catches outgoing and incoming messages, scans it and deem the message as being malicious or sent without users notice. Currently, SeraphimDroid only notifies the user about the danger and user have to take action. More advancement will be done in upcoming versions.

Application Locker

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 lock any application and unlock it. Whenever a locked application is started a password prompt is shown, on entering the correct password only the locked application can be accessed else the application will be terminated.

Service Locker

This is a protection mechanism from unauthorized use of essential services such as Bluetooth, Wi-Fi and Mobile Data. It can save the user from both malicious use, Bluetooth for instance, also cost from services like Mobile Data.

User can lock these services from the application. Whenever the state of these services is changed, either switched on or off, the user will be prompted for a password. If he's unable to provide the correct password, the service will be restored to its original state.

Geo – Fencing

Geo - Fencing is something of a new addition to SeraphimDroid. Enabling Geo-fencing create a virtual fence around the device's current location. If the mobile goes out of the range it starts performing some specific action which users selects while enabling the service. Also, user could enable location updates in case phone got stolen.

Remote Lock / Wipe

If user forgets to turn on the Geo-fencing and phone gets lost this feature can come in handy. This allows user to send a secret code to the user's device which activates the service. The phone then lock the phone, wipe the user's data or send the current location of the device or all of at once.

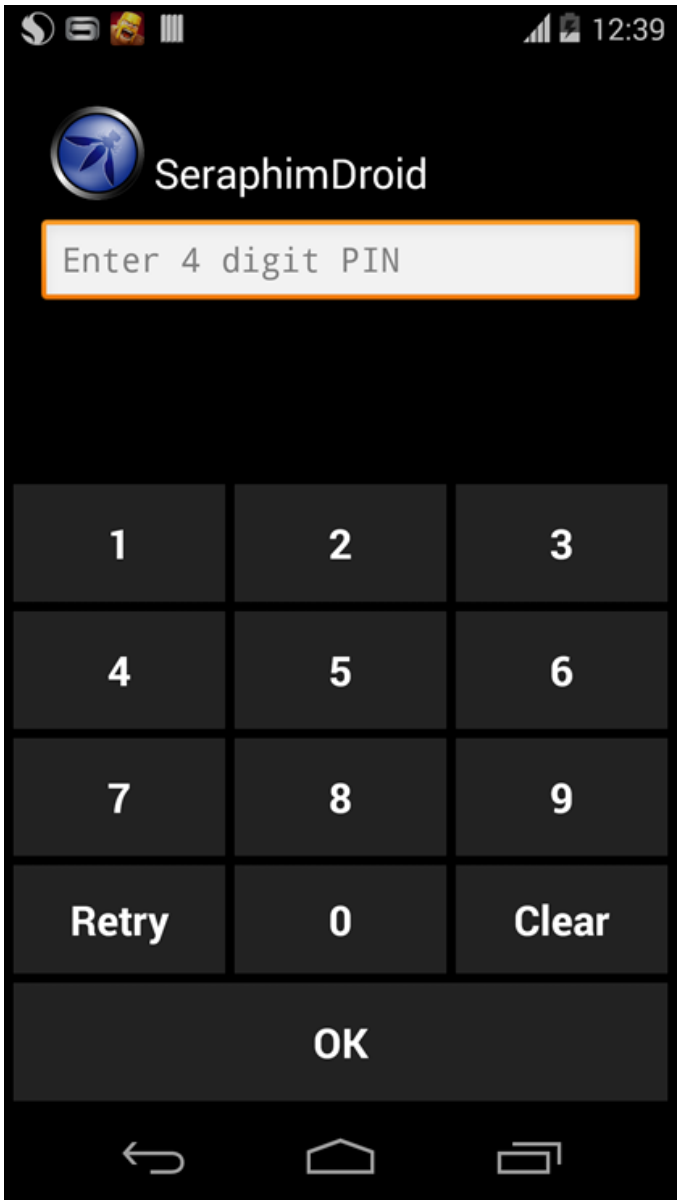
Knowledge Base

This Section is the latest introduced feature in the Application. Under this Section, Different Article are listed related to this App and General Security of your Droid. The Articles are well detailed and are fetched from a Backend REST API, deployed on Openshift as a Sister Project of this Project. All the articles displayed belong to a particular category, like General, Security etc. New Articles are published by the writers on Educate Knowledge Base.

Usage

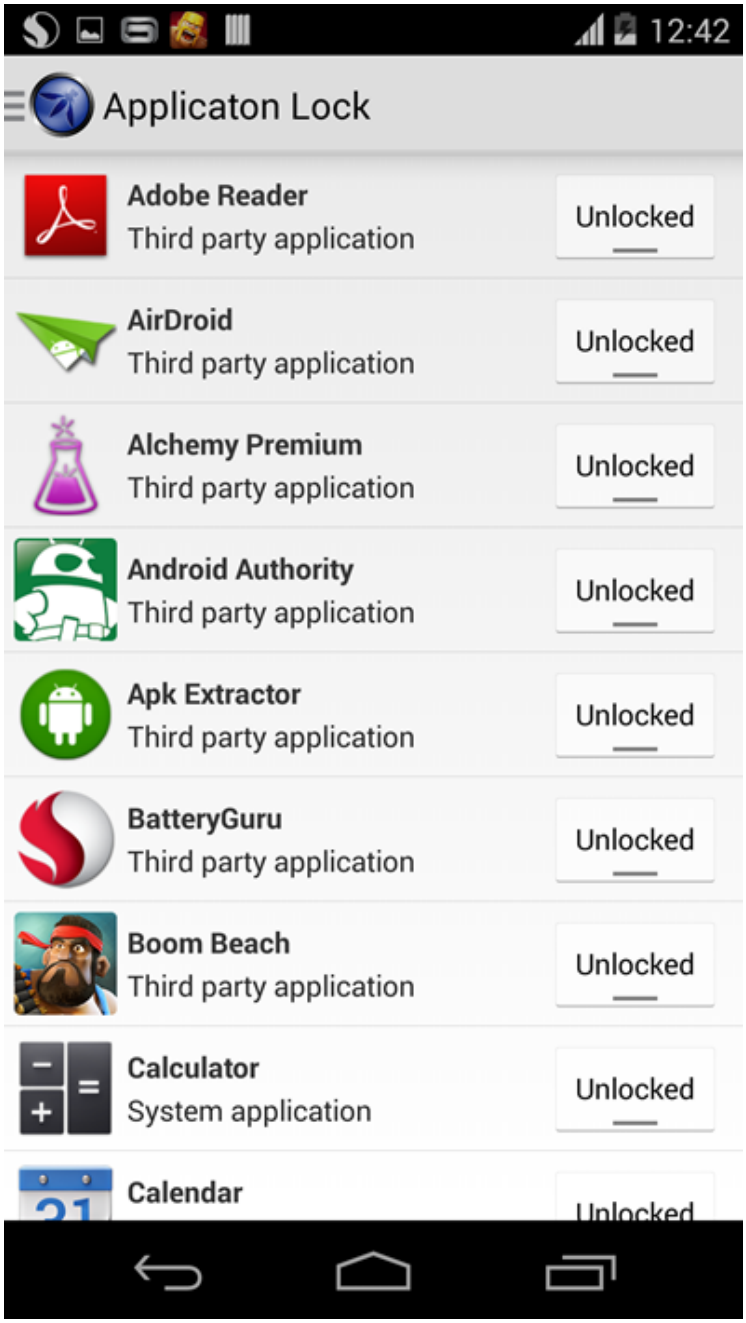
First Start

Before SeraphimDroid can actually be accessed, user needs to create a PIN code to lock the application. The same code will be used to unlock locked applications. The process to create a PIN is really simple. When SeraphimDroid is started for the first time a prompt is displayed to create the PIN which looks like the image below



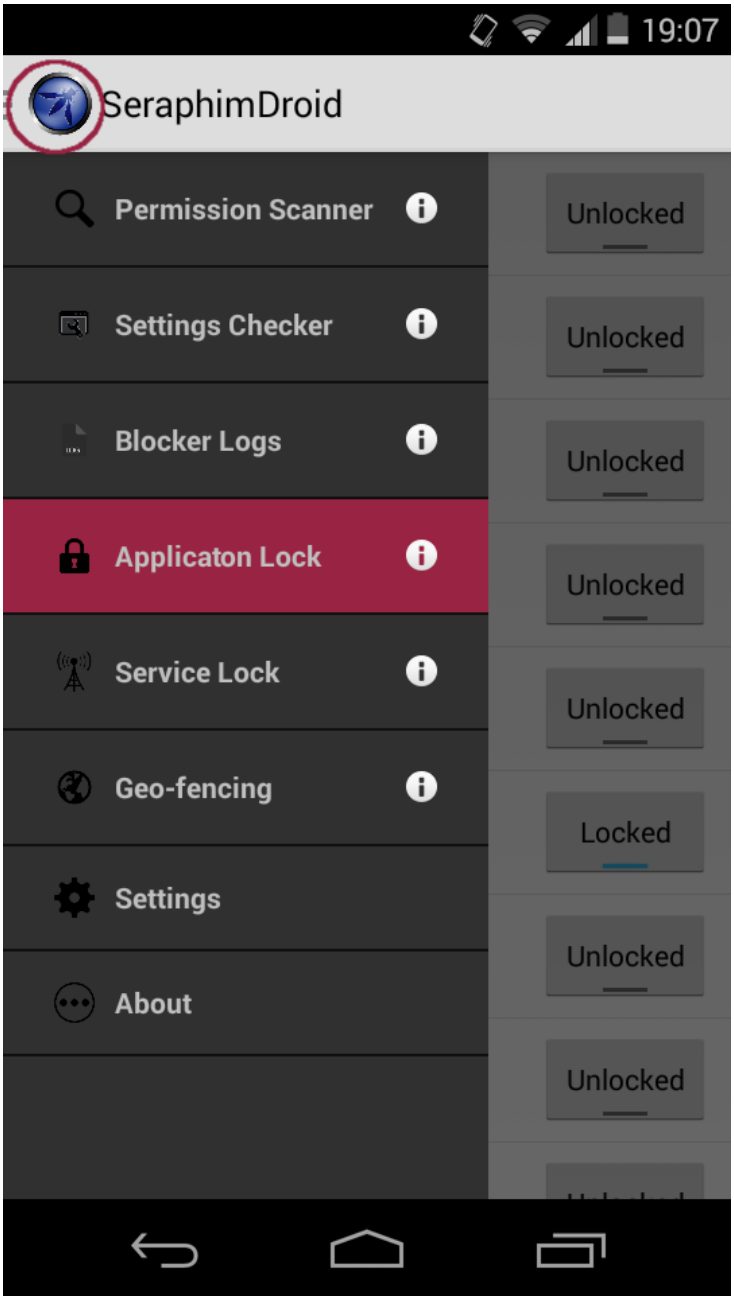
The PIN needs to be entered twice to make sure the user enters the correct PIN. Once the PIN is created user will be asked to enter it every time SeraphimDroid is launched. ***The PIN needs to be at least 4 digits long.***

After the access is granted for SeraphimDroid, you will see the Application locker, with the list off all the installed application that could be locked, just like in the image



Navigation

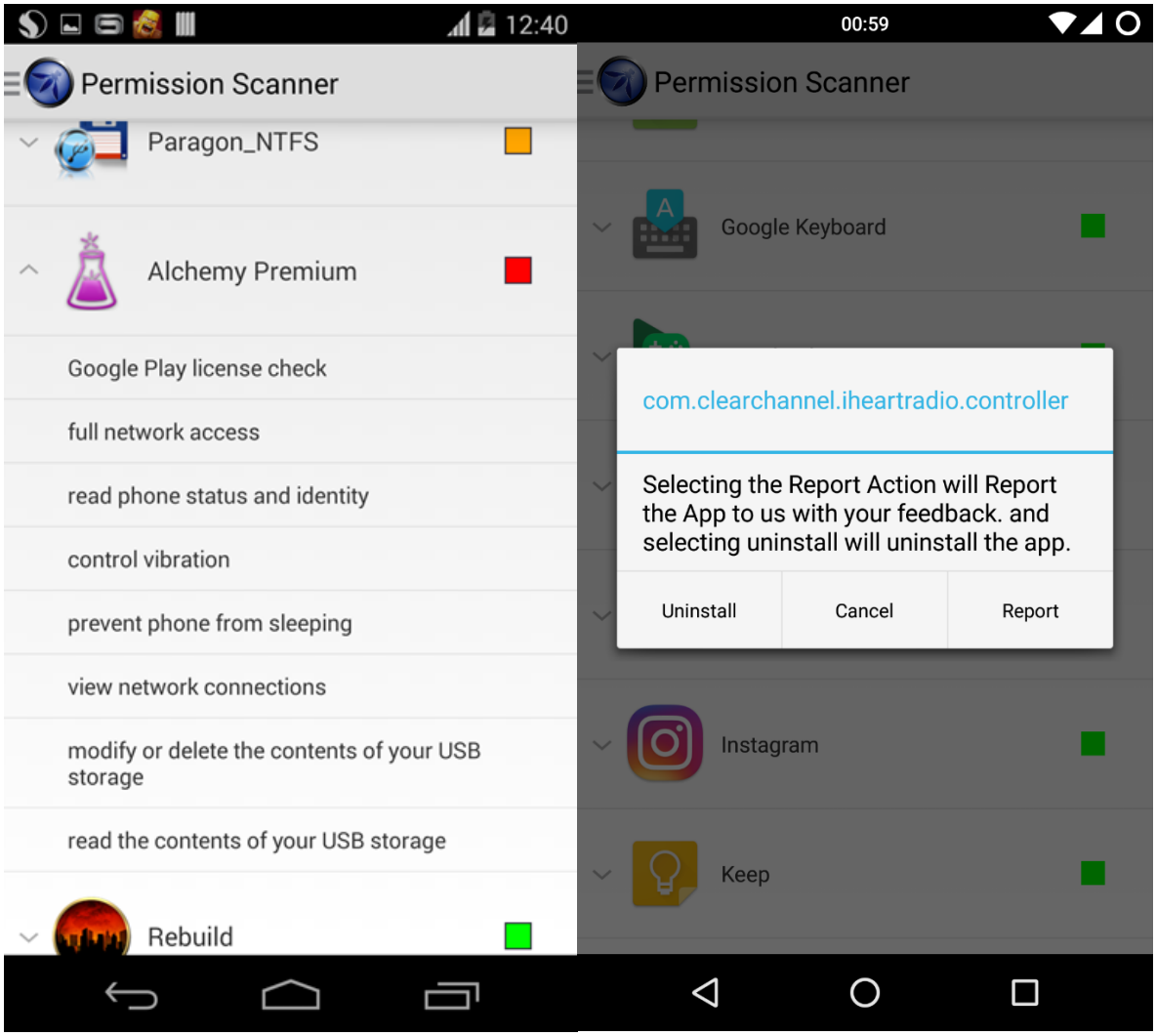
SeraphimDroid is pretty easy to use, all the features can be accessed using the navigation drawer. The navigation drawer can be access either by sliding from left or by tapping on the app icon in the action bar as shown in the image below.



In the navigation drawer you can see all the services that SeraphimDroid provides. Use of each of the service is provided below. In the application, user can see a brief introduction for each service by tapping on the info icon. For some features, we have articles published in the Knowledge Base so the user is taken to the Relevant articles for that section.

Permission Scanner

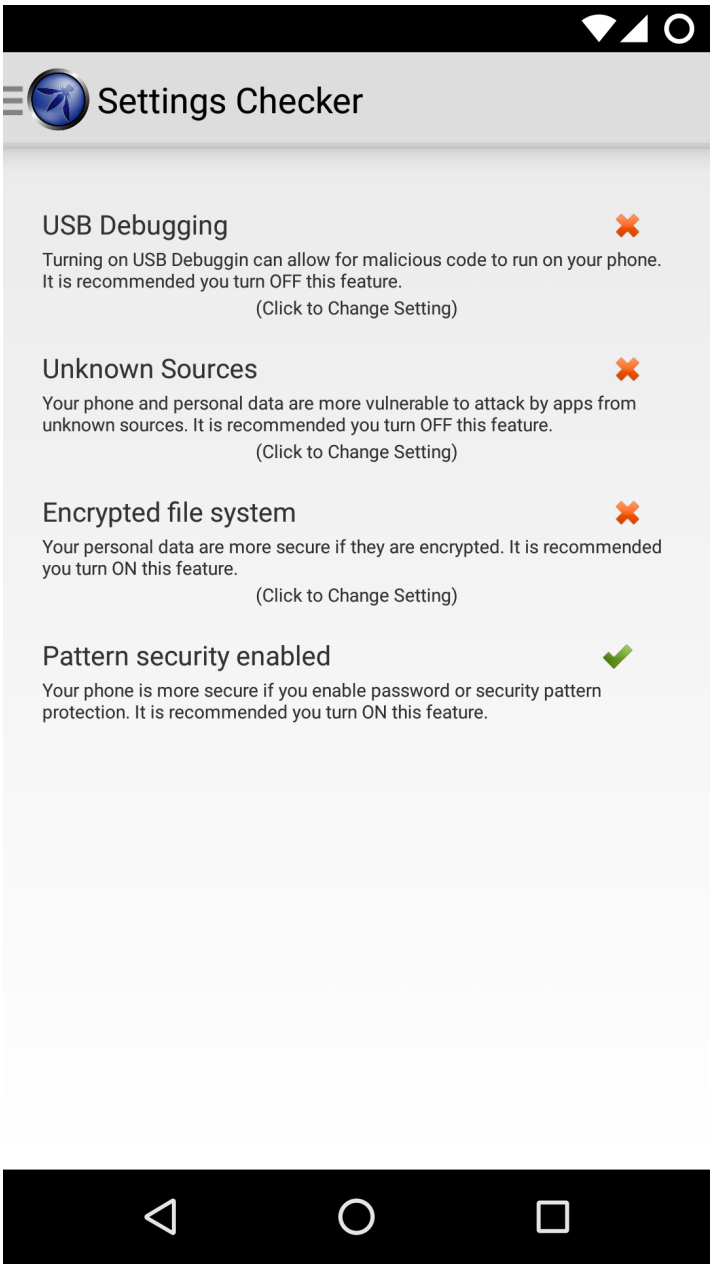
Permission Scanner is the first service that SeraphimDroid provides. It scans all the installed application and display its danger level using colour codes, as mentioned in above section. Expanding any application user can see what permission that application uses. A description about the permissions intended use and malicious use is also provides within the permission scanner.



User can see the description by tapping on the permission and a dialog will be displayed showing the details about that particular permission, which includes the general use for that permission and malicious use as well. User can also report the Application or Uninstall the Application from the Dialog shown on Long Press for the Item.

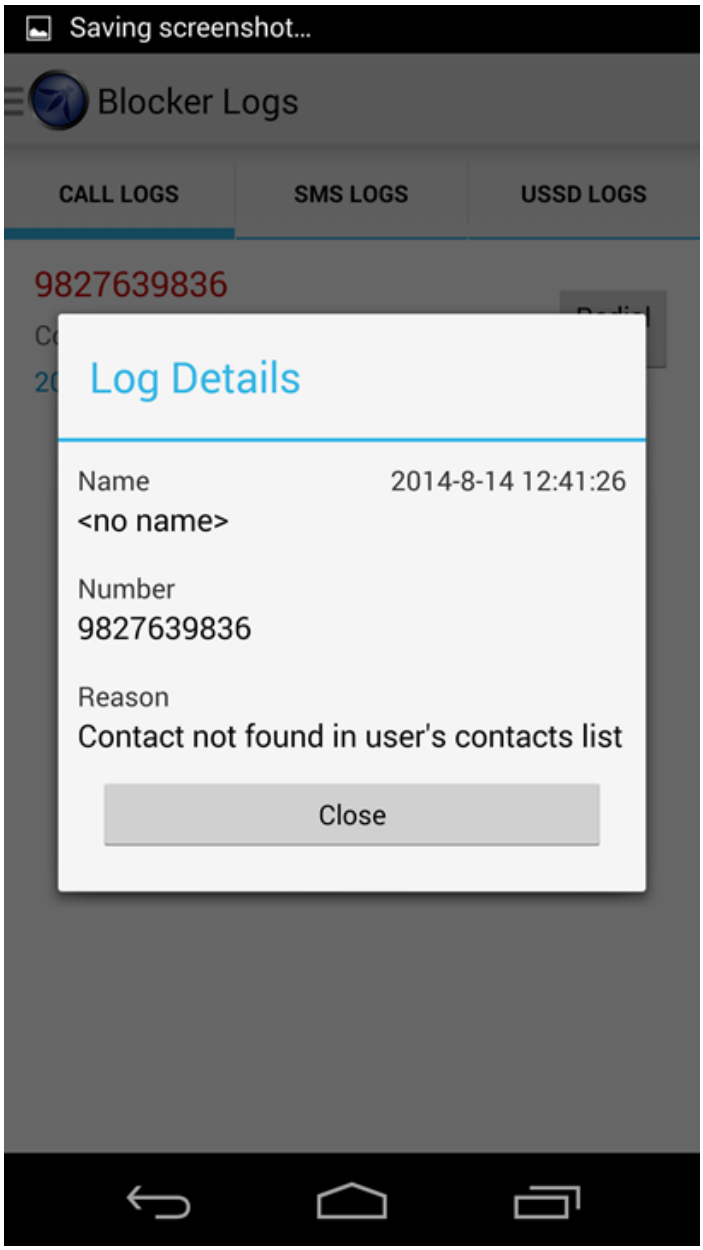
Settings Checker

The next service in the drawer is the Settings Checker. This displays the device's settings, which are prone to malicious activity if not set to its recommended state. The one which are not set to its optimal state, a red cross is shown, and also a “click to go to settings” option which will take the user to the respective settings screen where he can change the setting. The options which are set to the recommended setting, a green tick is shown. The screenshot below shows the Settings Checker Fragment. The Settings Checker features various settings checks like, Unknown Sources, Pattern Lock etc.



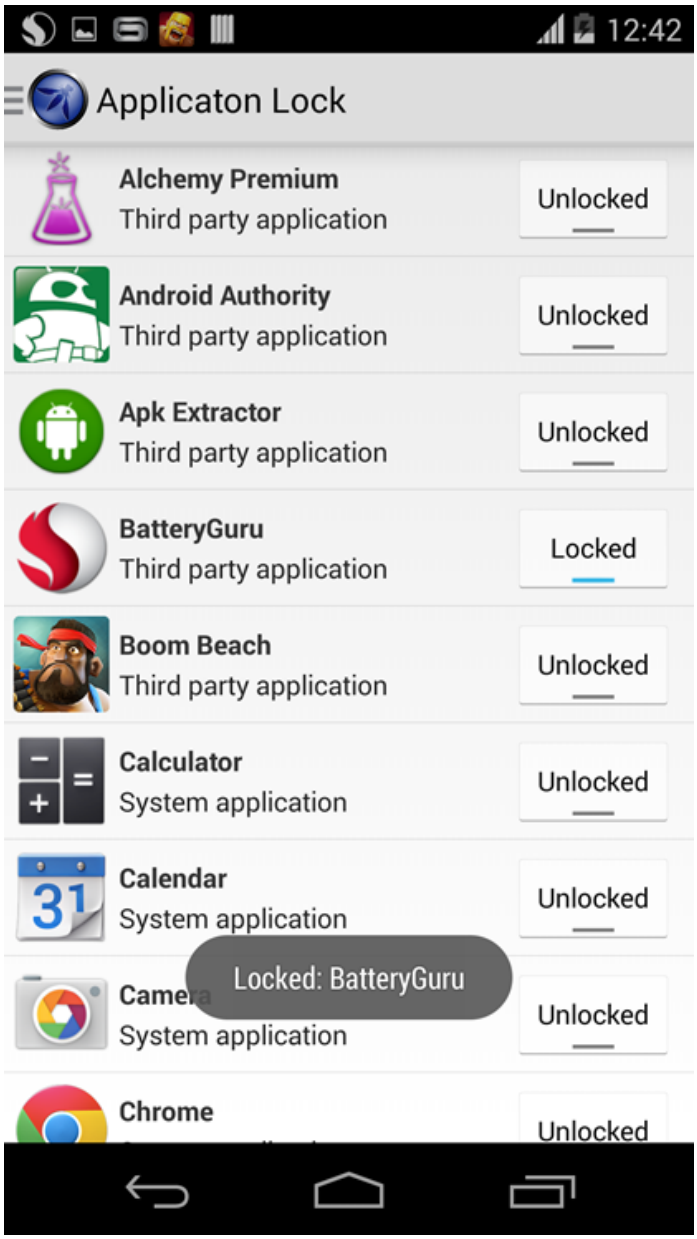
Blocker Log

The next service in the drawer is Call blocker and SMS Interceptor. The Blocker log displays all the logs for blocked calls, malicious SMSs and harmful USSDs. The log displays useful information for the user about the blocked call (for example time of call, number called etc.). Tapping the log item shows more details about that particular log.User can swipe between tabs or tap the name of the tab to view details about other logs (SMS Log and USSD log). The navigation kept as simple and as user friendly as possible. A sample for the log is shown in the screenshot



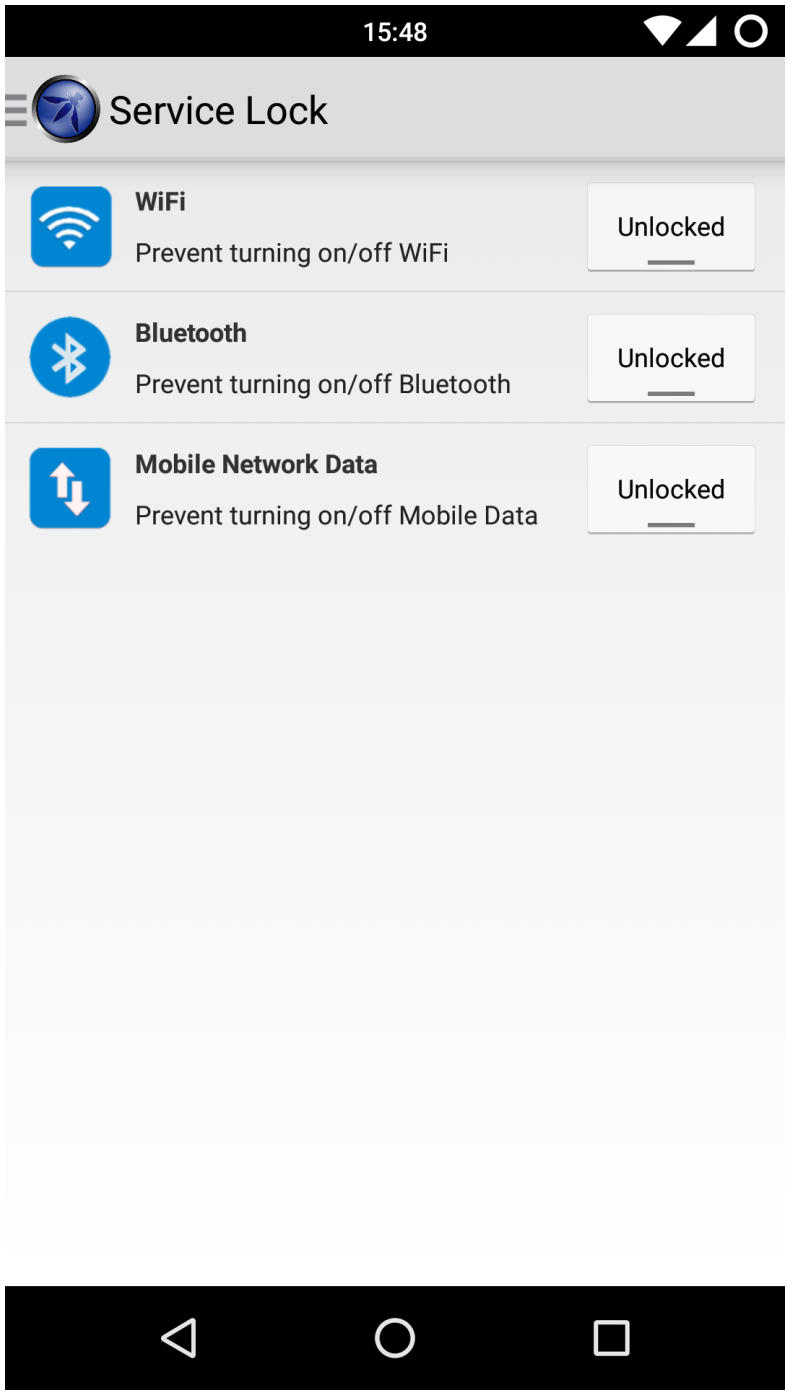
Application Lock

Going down the list of service the next on is Application Locker. Quite easy to understand the use and even more easy to use. All user needs to do is lock the application he wants to protect and the work is done. Any time the locked application is launched, the password prompt is displayed on the screen, which prevents the access to the locked app. Only on providing the correct PIN code can the application be accessed. The interface is pretty much simple and is shown below. The screenshot also displays one of the application being locked.



Service Lock

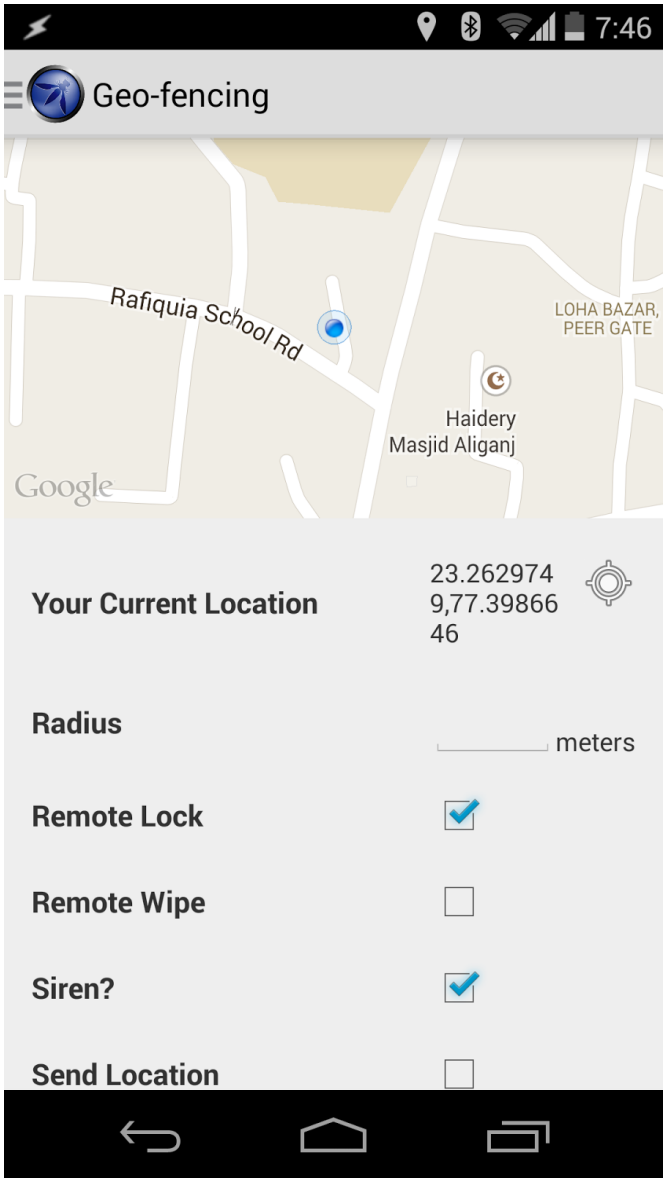
Much like the Application lock is used to lock target applications, The Service Lock is used to lock essential Android services, such as Wi-Fi, Bluetooth & Mobile Data. Whenever a user tries to change the state of any of the above locked services, SeraphimDroid will prompt for PIN, and only upon successfully entering the PIN shall the state be changed. Otherwise, the service will be restores to the previous state. Below is a screenshot of the Service Lock Fragment.



Geo-Fencing

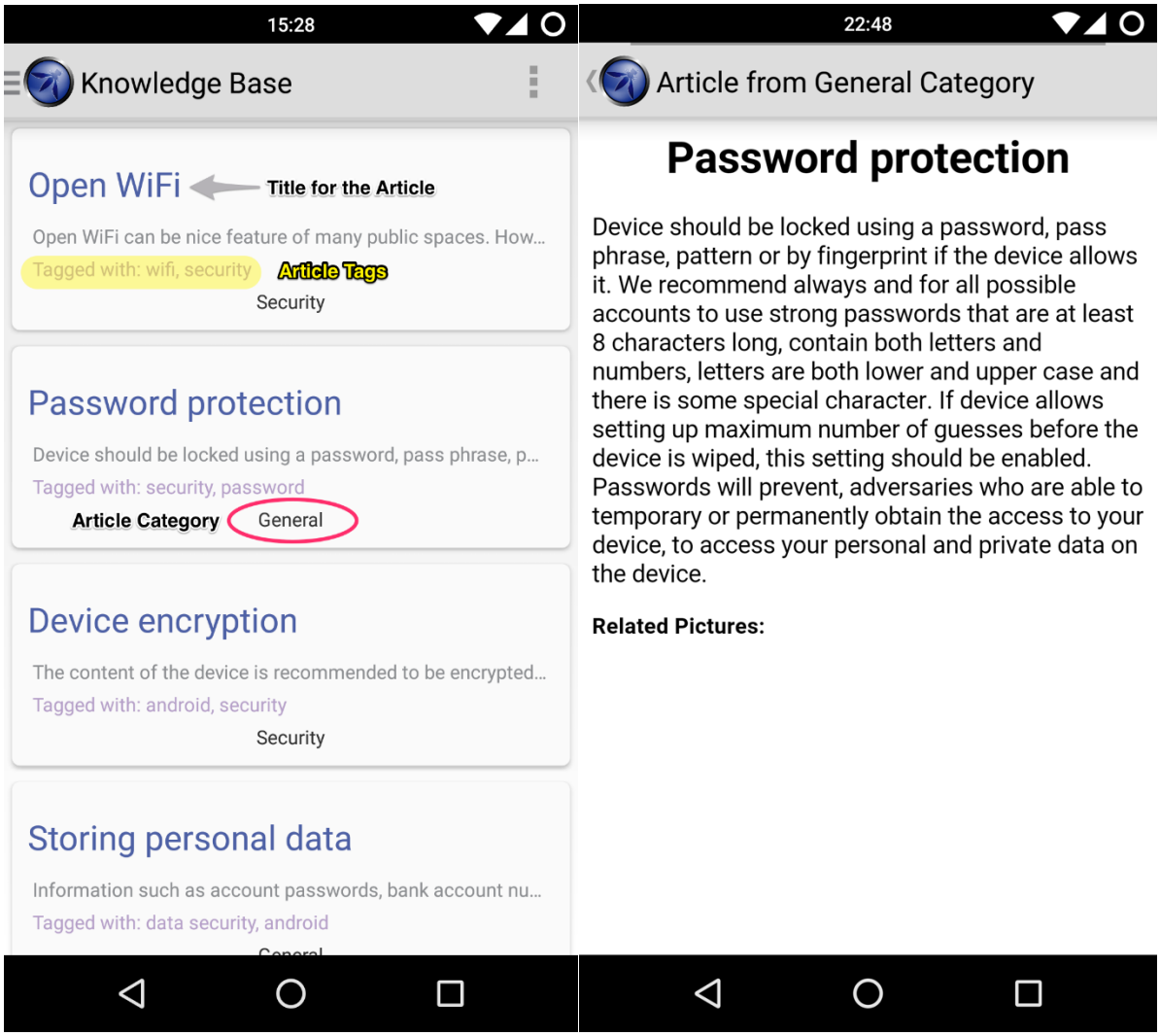
Geo-fencing contains a Google Maps to show user his current location. Then there is a button to get his current location for the service to start. Then follows the range for the perimeter, it can't be less than 200m because the precision of GPS is not so accurate. After that there are four check boxes, one for enabling each feature i.e. lock phone, wipe data, siren and send location.

The service won't start unless the GPS is on so in case user does not turn the GPS of the device on a prompt is shown, and if user cancels that prompt, then the button for starting the Geo-fencing is changed to display GPS prompt. Only when the GPS is turned on can the service be enabled. This provides better GPS tracking and location accuracy. The screenshot for Geo-fencing is the below image.

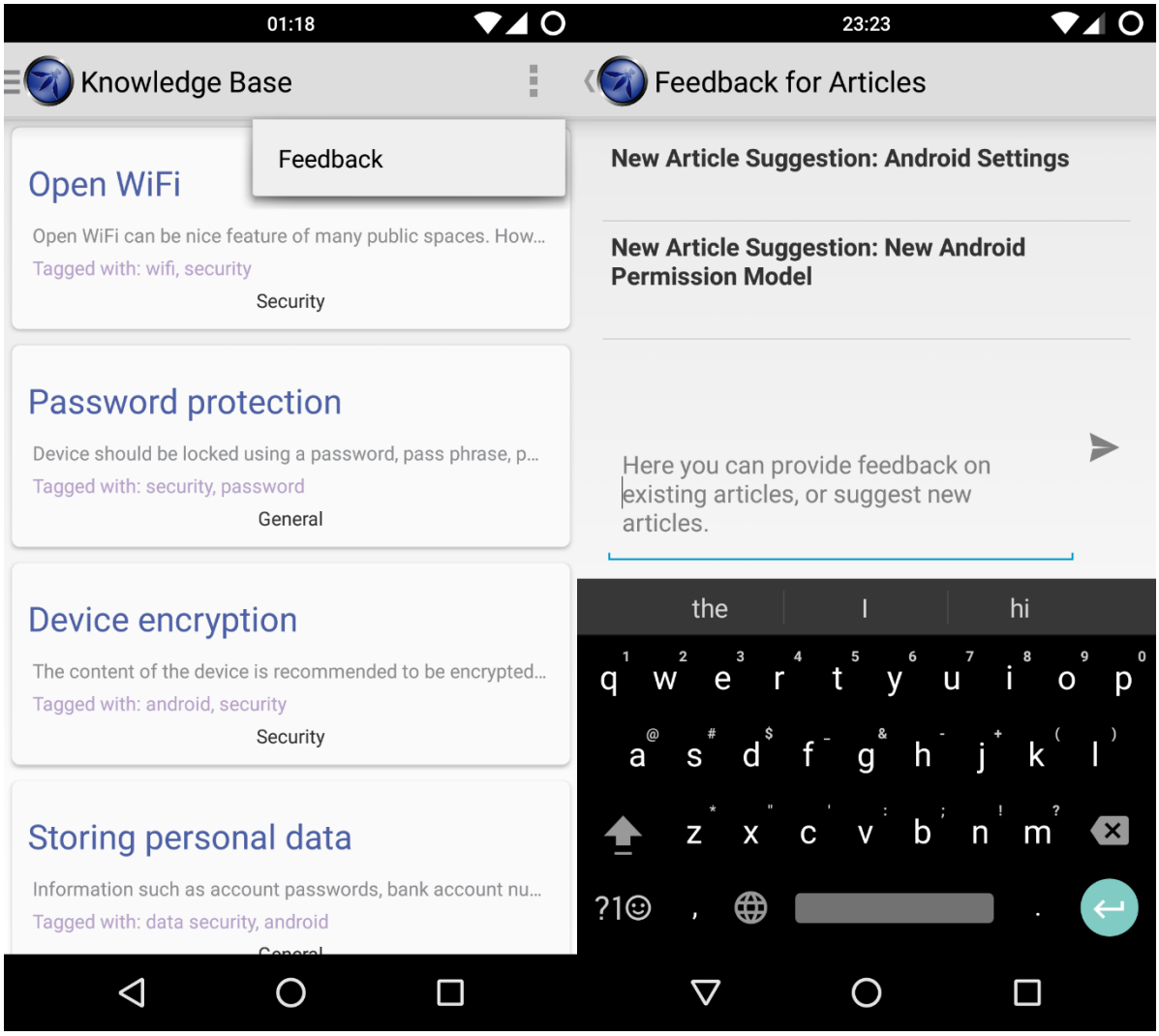


Knowledge Base

This Section is the latest introduced feature in the Application. Under this Section, Different Article are listed related to this App and General Security of your Droid. The Articles are well detailed and are fetched from a Backend REST API, deployed on Openshift as a Sister Project of this Project. All the articles displayed belong to a particular category, like General, Security etc. New Articles are published by the writers on Educate Knowledge Base. The articles can also be tagged with multiple tags on basis of which they can be filtered.



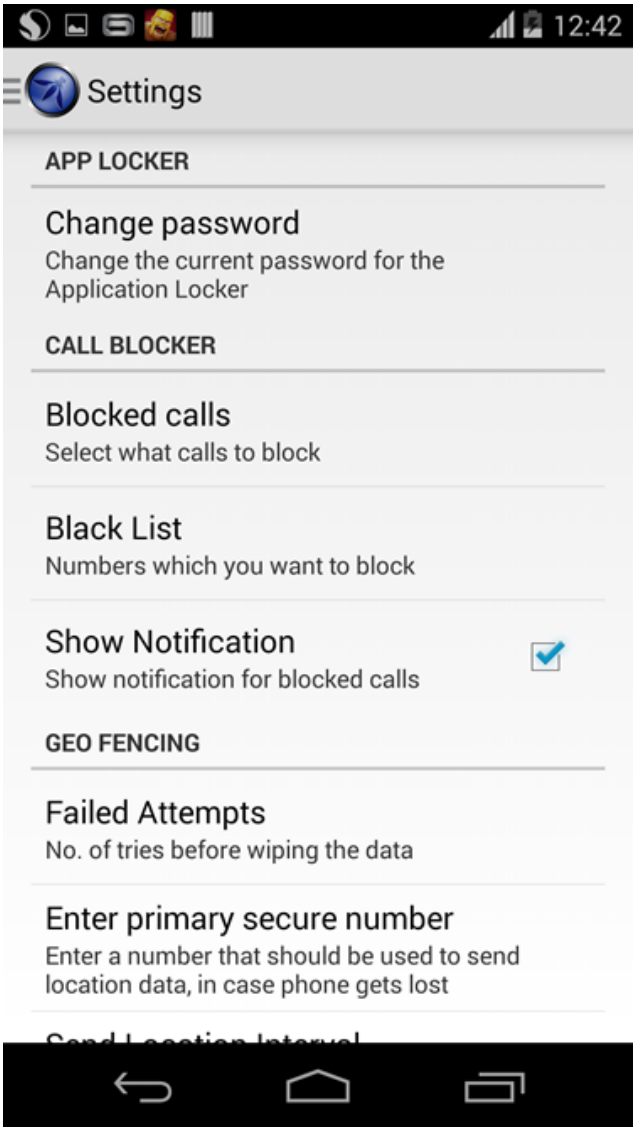
The articles are also available to read offline once they are downloaded i.e. opened. The articles are opened to the last state they were updated and are updated whenever you next time go Online.



Users can also provide feedback on existing articles and provide Feedback for Existing Articles from the Options Menu.

Settings

The settings is next in the drawer menu, this is the place for setting preferences for the SeraphimDroid. Here user change the PIN code of SeraphimDroid, he can set the category of calls that should be blocked and add numbers to blacklist to block those particular numbers. The settings page also contains information regarding the geo-fencing, user can set secure number, the number of times after locking the data should be wiped and the interval with which the device should send its current location. The user can also have a look at the Blocked Numbers and calls that the user wants and also have a look at the Black list that list permanent rules for blocking calls on through Seraphimdroid. This Section also lists an option for in-App Notification for the Blocked call and Malicious messages.

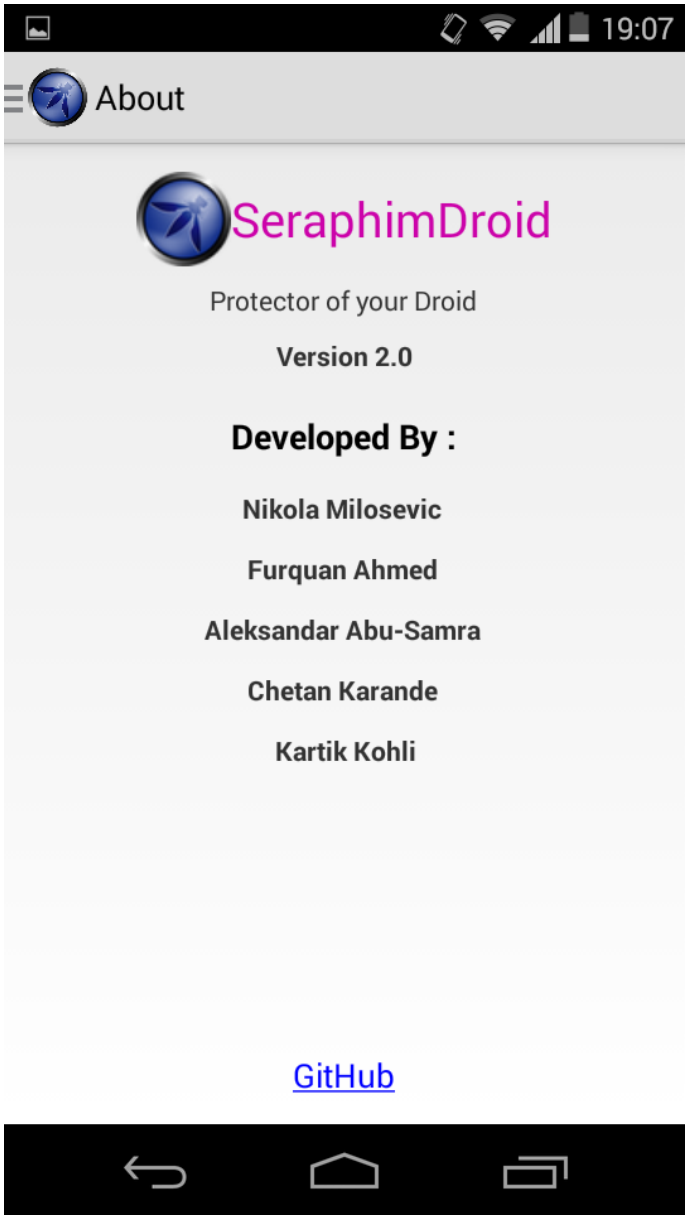


The remote service preferences are also accessed from the setting fragment. These include remote lock, remote wipe, remote location and remote secret code. Remote Secret code is set by the user to trigger the remote services. There services are disabled by default,

user needs to enable these services before the secret code trigger could work. The User can also list or state the Failed attempt count and primary security number for the Remote Locking Wiping Section.

About

The about fragment contains the more information about the project. It has the link to the project page and the code on the GitHub. Also it shows the names of the developer who contributed to the project along with the name of the owner of the project. The version information is also displayed in the same fragment.



Conclusion

SeraphimDroid helps the user to understand the android security architecture more by letting him to the insights of the access modes used by application to request some services. These services are only allowed if user allows them which makes user responsible for making choices before installing applications. This might be a good practice but a general user doesn't actually seem to know about all the details, SeraphimDroid provides this details.

Along with the documentation SeraphimDroid also provides some security and privacy features which helps user secure his phone from theft and also from malwares. The best part it does is alert the user about the money costing apps and saving users money.

Overall the application is functional and is useable but it's a software and there is always possibility for it to be improved. In its latest update, SeraphimDroid uses state of the art Machine Learning algorithm to classify apps into "Malware" or "Goodware". An online database can also be created with the list of all the harmful application names which could cause user harm, this list will be created by people reporting the malware apps.

Also the SMS detection could be improved and in current version the SMS is rated harmful if it contains unsaved phone numbers which could be improved again by having a database containing the details about the malicious SMS.

Furthermore, a widget could be created to enable or disable the Geo-fencing with the touch of the button. This will make it really easy to enable the anti-theft feature of the phone. That's all.