Today I have to make one very important announcement. The first version of OWASP Serphimdroid has been officially published. It is now publicly available in Google play store (https://play.google.com/store/apps/details?id=org.owasp.seraphimdroid). I would like to tell a bit of the background of this project and describe some main features here.

It has been about a year ago when I started this project. I had an idea about building quite simple android security application that would not rely on some large database or some malware labs, but rather protect users through a set of heuristics that will at the first place prevent them from loosing a money through detecting if some malicious application is trying to send premium SMS or perform some premium calls. Then the idea expended a bit. We also thought that it would be nice to educate users about dangers coming from some of the android permissions. And at the end it expanded to anti-theft protection as well.

There was some efforts made at the beginning of the project, mainly on research how to implement these things. The project was quite in incubator phase which included a lot of research. However, since it is an open source project, without any finance, we were doing it on a spare time and it went quite slow.

In order to accelerate the project we applied as a part of OWASP (Open Web Application Security Project) to the Google Summer of Code. There is very nice policy in OWASP that every project, even the very tiny as this was, especially compared to the OWASP ZAP, get at least one student allocation. So here I would like to thank both Google and OWASP Foundation for supporting the project in the right way.

For our project there was 3 students that have sent an application. Our choice was student named Furquan Ahmed. He decided to redesign the application and add some new features such as application locking, remote lock and wipe and theft protection. During the summer he did a great job crafting our first version of OWASP Seraphimdroid security application. It was very good working with Furquan as a project leader and Google summer of code mentor. Regarding all the problems different mentors were mentioning on the mailing list, we had none, it all went quite smoothly. And now finally it is on Google play published as a first version. However, there are a lot of plans. Settings checker has to be implemented. Also we are waiting for the user's feedback as well. And as always I would like to invite anyone who is interested in contributing in any way (now as it is published, we still need coders, but also people who may take care of publicizing the project).

Main features

OWASP Seraphimdroid is a privacy and security protection app for android devices. It enables users to protect their devices against malicious software, phishing SMS messages, execution of dangerous USSD codes. OWASP Seraphimdroid also enables users to keep their device safe from theft or loosing with its geofencing feature. OWASP Seraphimdroid has two aims:
- To protect user's privacy and secure the device against malicious features that may cost user money
- To educate user about dangers coming from certain android permissions and setting misconfiguration
In order to achieve these security, privacy and educational aims we have built a set of features and will be periodically introducing new security features.
Features:
* Application locker. With OWASP Seraphimdroid you may lock access to certain or to all of your application with password
* Permission scanner. Permission scanner will show you the list of all installed application and the permission they are using. Also app will describe potential malicious use of certain permissions. Seraphimdroid will sum up the danger factor for all of the permissions and indicate whether the application may be considered potentially dangerous.
* Incoming SMS blocker. This feature will scan all incoming messages and alert user if it find in the content potential phishing
* Outgoing SMS scanner. The application will monitor outgoing SMS and alert user if the some of the application is trying to send SMS. This is the usual scenario how malware creators earn money - by sending premium SMS messages.
* Outgoing call blocker. This feature will allow you to perform normally outgoing calls, but it will block outgoing calls performed by other installed applications. Similarly to outgoing SMSes, this is the scenario malware creators use to earn money.
* Geo-gencing. This feature allows user to set a location range where the device should be. If the device exits the range it may set up alarm or start sending messages to the defined number with its location.
* Remote location. If you lost your phone, you'll be able to send SMS with a defined secret code as a content and your phone will reply with the location coordinates of the device.
* Remote lock. Similarly, you may lock your device using a message with secret code
* Remote wipe. If your phone is stolen, you may send a message with secret code and wipe all user data from the phone.
As all OWASP projects are open source project, this one is no different. It is published under GNU GPL3 licence. Official OWASP page for the SeraphimDroid security is [https://www.owasp.org/index.php/OWASP_SeraphimDroid_Project](https://www.owasp.org/index.php/OWASP_SeraphimDroid_Project)

Source code of the project may be seen here: [https://github.com/nikolamilosevic86/owasp-seraphimdroid](https://github.com/nikolamilosevic86/owasp-seraphimdroid)


Once again I invite you to try app, if you are interested in contributing, don't be shy, contact me. I hope you will enjoy the app and definitely with it on your phone, feel more secure.

All rights reserved and copyrighted by inspiratron.org and Nikola Milosevic