[Inspiratron.org - Natural language processing, machine learning and cybersecurity](https://inspiratron.org)

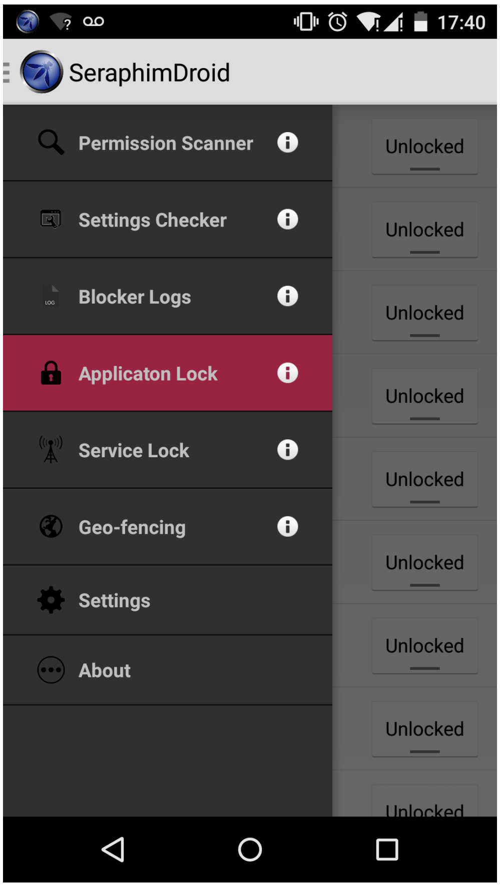
New version of OWASP Seraphimdroid (v2.0) is published

by Nikola Miloševi? - Tuesday, September 08, 2015

https://inspiratron.org/blog/2015/09/08/new-version-of-owasp-seraphimdroid-v2-0-is-published/

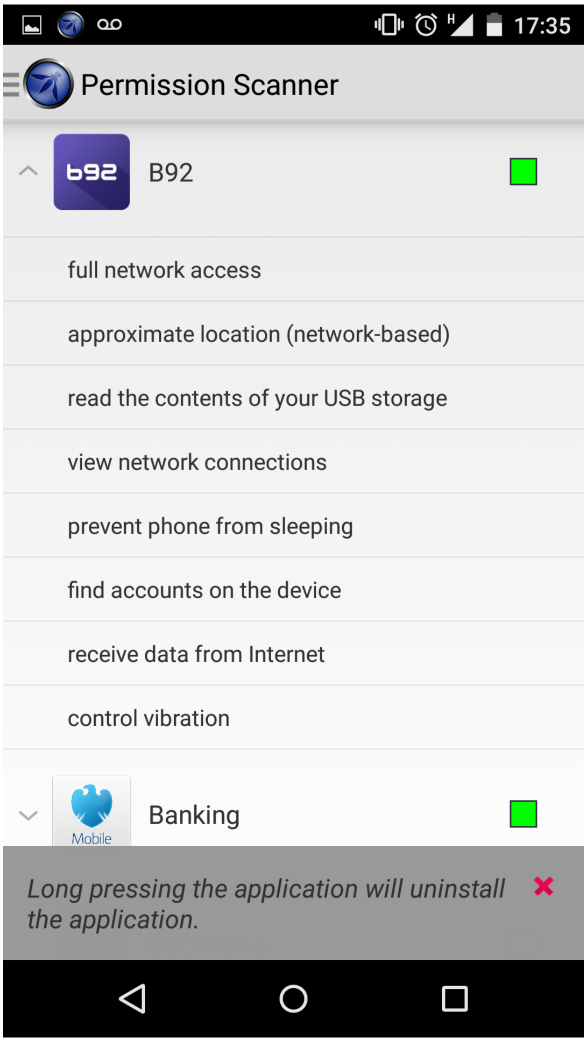
Dear users and security aware people, we have a great announcement. The new version of OWASP Seraphimdroid is published with some very interesting breakthrough features. If you liked OWASP Seraphimdroid before, now you will probably love it. We have improved machine learning aided permission scanner, new settings scanner, improved SMS interceptor, improved application locker, and some more. OWASP organized OWASP Code Summer Sprint, where OWASP Seraphimdroid participated as one of the project. Student that was proposed some and was selected to develop improvements on OWASP Seraphimdroid was Kartik Kohli. I had opportunity to mentor him as OWASP Seraphimdroid project leader. So let’s start explaining the major improvements.

If you are not aware or do not know what features had first version, you can remind or inform yourself here.



Permission scanner

We had permission scanner in the first version, but it had flaw that if application is using too many permissions, it would alert that application might be dangerous. Basically, previously we assigned weights to permissions and summed them. We assigned thresholds to red and yellow alert. This was one of the simplest solutions, but now we have much improved this algorithm and it probably took most of the development time during OWASP Code Summer Sprint. It gave a lot of headache: how to tell user whether application is potentially malicious or not, just based on permissions. We thought about several rule based solutions, but almost every had an obvious flaw. Solution that came out was to use some of the malware/goodware datasets and try to train machine learning dataset. On one of the OWASP Manchester meetings, I met dr Ali Dehghantanha, lecturer on Salford University, who provided us android malware/goodware dataset his research group compiled (http://www.alid.info/blog/2015/2/4/android-malware-research-dataset). We used this dataset to make machine learning model. We tried several machine learning algorithms including Support Vector Machines, Naïve Bayes, C4.5 decision tree and random forests. The best results gave us Support Vector Machines (SVM) with Sequential Minimal Optimization (SMO). The F-score we got was 87.9%, with both precision and recall giving same performance, using 10-fold cross validation in Weka toolkit. This performance is not perfect, but it is much better than rule-based approach we had and it also is comparable to some anti-malware tools on the market. Also, it is able to detect zero-days malware, since it model behavior, rather than its exact signature. Having look on report by Cyveillence, which reported in 2010., that only 19% of malware can be detected on the day when they are released by antivirus vendors, we believe that 87.9% is quite an improvement, especially that this was made on unseen malware. However, there might be some mistakes, since performance is not perfect, so we would leave up to user, whether he want or not to remove the application. Also, there is no more yellow alarm, we now have binary classification whether application is malicious.



Permission Scanner

B92 🟩

full network access

approximate location (network-based)

read the contents of your USB storage

view network connections

prevent phone from sleeping

find accounts on the device

receive data from Internet

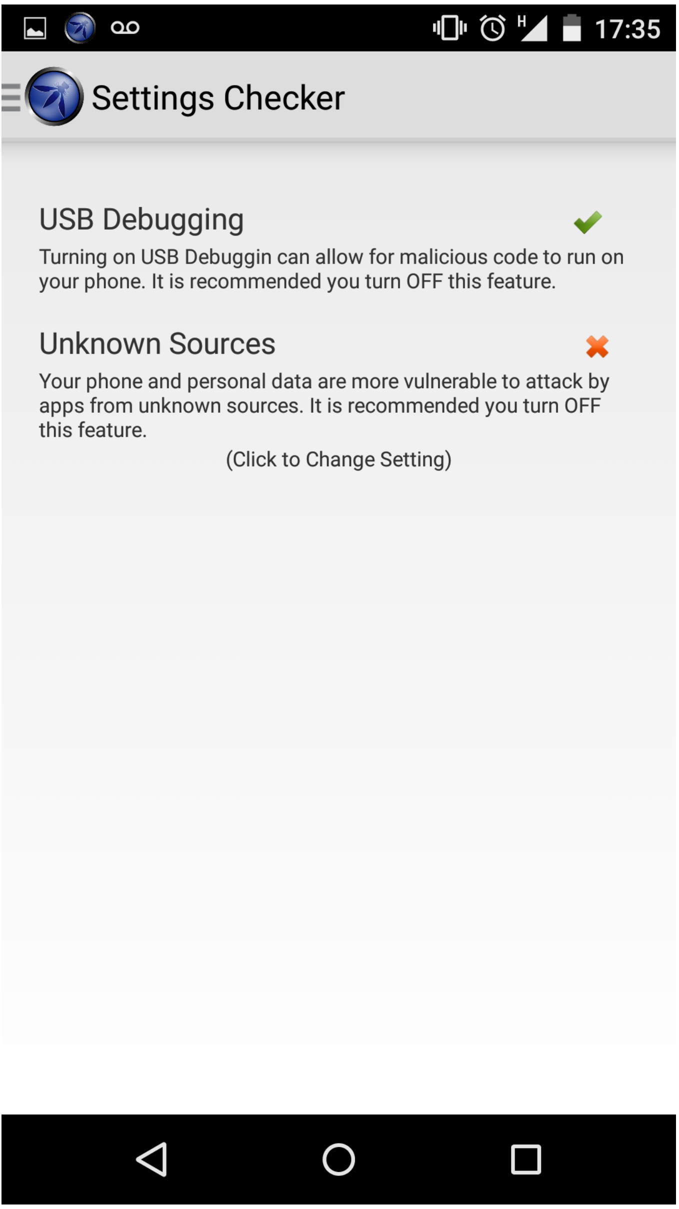
control vibration

Banking 🟩

Long pressing the application will uninstall the application. ✕

Settings scanner

This is completely new feature in OWASP Seraphimdroid. However, this is quite standard tool in mobile anti-malware community. This feature periodically (default is once a day) checks whether the settings on your android device is set securely by recommendation. If it is not, the application will fire a notification. User can click on unset permission and application will open settings, so user can change the problematic setting on his or her phone. This feature, we believe will make another layer of protection to our users and make them feel more



USB Debugging ✓

Turning on USB Debuggin can allow for malicious code to run on your phone. It is recommended you turn OFF this feature.

Unknown Sources ✗

Your phone and personal data are more vulnerable to attack by apps from unknown sources. It is recommended you turn OFF this feature.

(Click to Change Setting)

safe.

Service lock

Another new feature that enables you to lock services such as WiFi, network access and Bluetooth. If the feature is enabled, on attempt to enable these services password screen is shown.

SMS interceptor

This is actually bug fix. OWASP Seraphimdroid used to fire notification even if SMS was sent by Google Hangouts. This bug is now fixed and OWASP Seraphimdroid will now fire notification, only if SMS was sent by non-default application.

Installation locker

This is a new feature that is available to turn on in settings. You may enable lock screen to show whenever someone tries to install or uninstall some application on your device. Quite useful tool for controlling what is on your phone and what people you share your device (children, family or friends) with may or may not do.

SIM Change listener

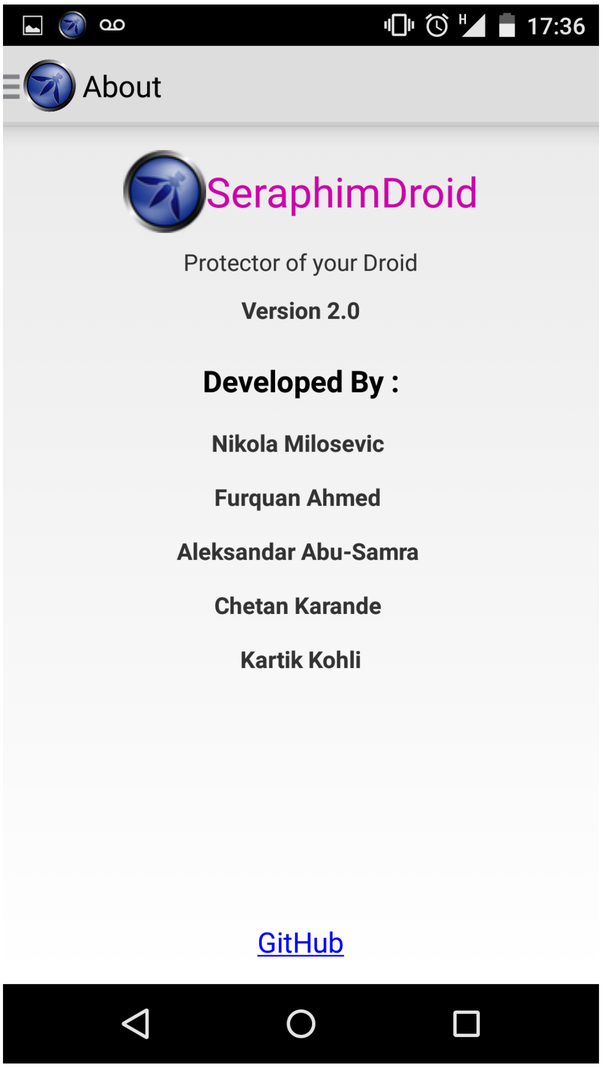
This is completely new feature. Seraphimdroid listens whether SIM card is changed and if so, it will prompt Seraphimdroid Password screen. We believe that this feature will prevent thieves to change SIM card and use the device. Without password or system flashing (for which is needed special equipment and professional knowledge), device would not be usable. It will also send the IMSI (International Mobile Subscriber Identity) number, which is SIM card related info and which can lead to the capture of thief, to the phone number user set as security number where he wants information about phone (location, IMSI, etc.) in case the phone is lost and event is triggered (either by sending SMS with special code indicating the loss of phone or by phone exiting geographical area user set, or by change of SIM card).

Application locker

This was also bug, since on android lollipop application locker stopped working, since class we used in previous version became obsolete. Now this issue is fixed.

Conclusion

I hope you would like our improvements. If you have any comments and suggestions, please contact me. You can download the application on Google play



SeraphimDroid

Protector of your Droid

Version 2.0

Developed By :

Nikola Milosevic

Furquan Ahmed

Aleksandar Abu-Samra

Chetan Karande

Kartik Kohli

GitHub

Please let us know how you like it and what features would you like to se in future.