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

Introducing OWASP Seraphimdroid

by Nikola Miloševi? - Saturday, September 14, 2013

https://inspiratron.org/blog/2013/09/14/introducing-owasp-seraphimdroid/

About 2 months ago I started thinking about creating Android security application. I was looking where the other application are weak, since there are a lot of android device protection and anti malware application available on Google play. Thing I found that most of those application don't use application permissions as indicator that some other application is malicious. Other thing I also found is that a lot of features, that are quite easy to develop are premium. As I was looking for project to train myself, and help others to train developing android security tools that had not that luck to be employed by some anti virus company, I decided to create open source project. There will be no other interest involved, just to educate myself and other contributors how security and anti malware tools works on android platform, and also to provide free and open protection to our future users. One important part, to which I will return later, is also to educate users about threats that he or she may experience on their mobile devices.

Find a name, start a project

Next step before start of development was to find appropriate name for the project. Somehow Seraphim came to mind.

Wikipedia states following about seraphims:

> The word *seraphim*, literally "burning ones", transliterates a Hebrew plural noun; translation yields *seraphs*. Seraphs appear in the 2nd century BC Book of Enoch where they are designated as *drakones* (???????? "serpents"), and are mentioned, in conjunction with cherubs as the heavenly creatures standing nearest to the throne of God.

Definitely they are servants of God and protectors of Gods throne. So the name there Seraphimdroid came.

I am OWASP local chapter leader for Serbia, so I decided to register project with OWASP. They accepted proposition and created project page: https://www.owasp.org/index.php/OWASP_SeraphimDroid_Project

Also many other good things came from OWASP community. Since they project was published in OWASP connector, couple of guys emailed me wanting to know more about the project. Some of them are today contributors on the project.

On OWASP site is written the following:

> *OWASP SeraphimDroid is educational application for android devices that helps users learn about risks and threats coming from other android applications. OWASP SeraphimDroid scans your devices and teaches you about risks and threats coming from application permissions. Also this project will deliver paper on android permissions, their regular use, risks and malicious use. In second version OWASP SeraphimDroid will evolve to application firewall for android devices not allowing malicious SMS or MMS to be sent, USSD codes to be executed or calls to be called without user permission and knowledge.*

As I stated on the beginning I found out that not many security applications, available on google play, are paying attention on permissions.

Permissions are the root of Android security model, but it works out only if the users are educated enough. If user knows that a game does not need to send sms, and that function is indicator that the game is actually a trojan that sends most probably premium sms to some number and generates revenue for the trojan creators. Users are not often paying attention on what permissions applications requests when they are downloading apps to their device. Most of the other things are quite standard features that many different security apps do have. Lot of them don't have it together, so there is one more advantage of our application.

Development

Development started actually couple of weeks ago. There are four contributors so far, and they are listed on OWASP project page. I actually wanted to start with permission scanning mechanism, but for various reasons it turned up to quite big research task. Actually we have to research what combinations of permissions can be dangerous, and write down the article for each permission how it is usually used and how it can be misused for a malicious purpose. So I have started by accident coding incoming messages interception mechanism and checking if they can be phishing messages. Other guys did interception of outgoing USSD commands and interception of outgoing calls.

Outgoing USSD commands can be performed from the application and also by clicking on command in email or sms. It can reset device to factory settings, delete memory data, but also some of commands cost money. For now we just prevent commands that can damage device or data on device. We are looking for the list of commands that could cost money so we can prevent unwanted execution of that commands.

Some applications can call premium numbers and generate revenue for the developers of malicious application. We developed interception of all calls that are not in phone book. User may dial number that is not in phone book, but he or she will be alerted that number is unknown. Also application will notify user if some other application tries to dial some number.

Incoming sms are also filtered and checked if they might be phishing sms. If sms contains link or number there is possibility that sms is phishing. SMS of that kind will produce notification by Seraphimdroid, so user is warned that system detected possibility of phishing. When user reviews the message, he can click on Not phishing button, and SMS will appear as usually (this is still under development by the time of article writing).

This is where we are today. There are many other features on our roadmap, and we hope that we will publish first version on google play untill the end of year. But we still have to implement many features and protections.

Conclusion

If you want to suggest some features, please feel free to comment or contact me via email. I hope that you will like our try to make free and open source android security application via OWASP. I also hope that it will have reach at least as high as other commercial anti malware and security tools, and that this application will become standard in Android protection.