Personal Vulnerability Investigation Research Report

# Florin Pană – ICS4 – fall 2021

* **Introduction**

This research activity consists of investigating the vulnerabilities of the smartphone Samsung Galaxy J5 and deals with setting up and conducting vulnerability research of existing systems or technologies. This project activities have been done throughout a period of three weeks, in which I have conducted plenty of research and done some practical work as well, using the Kali Linux terminal.

* **Objective**

The main objective of this project is to find and explore the vulnerabilities of this particular smartphone by conducting rigorous research on the matter.

* **Strategy**

I have conducted the research and done the practical work for this project by keeping the DOT framework in mind. 3 of those strategies have been of good use throughout this activity:

1. **Library research – literature study**

Library research is done to explore what is already done and to determine what other theories could help me further in my design. I would always come back to my notes and the acquired concepts for a thorough re-examination. For example, while researching for this smartphone’s vulnerabilities, I have found some which have been fixed by the developer. I have only found that out after doing extra research on the matter and re-examining my findings.

1. **Lab research – prototyping**

Lab research is done to test parts or concepts of the product. I used lab research to learn if things work out the way I intended, or to test different scenarios. For instance, my research also has a practical side to it. I have created a virus designed to control the smartphone’s camera. Lab research has been useful in this side of the project.

1. **Workshop research – available product analysis**

Workshop research is done to explore opportunities. Prototyping, designing and co-creation activities are all ways to gain insights in what is possible and how things could work. This strategy also applies to the practical extra bit that I have done.

* **Findings**

Unsurprisingly, useful information on smartphone hacking is very difficult to find on the internet, due to the obvious security issues and because of the ill intended people. However, after rigorous research, I have managed to find the following vulnerabilities:

* There are software programs that can be used to spy the activity on somebody else’s phone: e.g.: Spyic
* There are software programs that can be used to unlock a phone without typing the password: e.g.: Dr. Fone

These software programs require a paid subscription after installation and the prices are substantial:

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

* There is a system bug on the older generation on Samsung smartphones, which can allow the attacker to unlock the password protected phone by bypassing the type password screen: accessing the emergency call menu and then pressing the home and power on buttons in quick succession. This technique can take a while to master since it requires high precision.

Graphical user interface, text, application

Description automatically generated

* Malware can find their way inside a smartphone via phishing, and they can do significant damage, such as erasing all the data, or they can simply be used to gather all the data.

This is a brief explanation of my attempt at creating a virus which can control the camera, take pictures, as well as get a history of the calls and messages:

This command creates a payload file named game.apk which needs to be installed on the victim’s phone:

A screenshot of a computer

Description automatically generated

Before the installation on the phone, the Metasploit listener must be turned on:A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

These commands have to be typed in the Metasploit console in order for the listener to start looking for a connection:

A screenshot of a computer

Description automatically generated

* **Project sub-tasks**

This subchapter addresses the subtasks found on the Canvas page of the project (<https://fhict.instructure.com/courses/11556/pages/explanation-personal-vulnerability-investigation?module_item_id=680296>):

* **Brainstorm about ideas and possibilities** -> Me and my teammates from the group project started brainstorming about several ideas for this project. After a few sessions, most of us have made our decisions. However, we have continued brainstorming even after that and as a result, me and another teammate have changed our target device. For example, I wanted to hack a toy RC car first, but then settled for the smartphone.
* **Make use of at least three strategies from the DOT research framework. ->** The explanation of how I have used the three DOT framework strategies can be found in this document, on page 2.
* **Define possible attack scenarios for the device or targeted device, app, or system. What would a bad actor or attacker want to achieve? Then for these scenario's investigate how and if this would be possible, by using combined research strategies and activities. ->** I have managed to come up with several attack scenarios, briefly described on page on page 2, on the findings chapter. As for what the attacker would want to achieve, there are several options: the attacker could have stolen a phone and now wishes to have control over it by bypassing the password. Also, by using malware inserted in the phone via phishing, the attacker could spy on the victim’s phone activity and could gather all sorts of information, from messages to pictures and other sensitive information.
* **Develop yourself on the required hacking techniques, possible exploit techniques and known vulnerabilities**. -> The development process is defined by my attempt at creating a virus on my kali Linux virtual machine and deploying it on my old smartphone using phishing. The technique was to send a link via email, which would automatically download the application.
* **Does a responsible disclosure policy exist for the object or subject you are considering\*? ->** No, this is information available online, not discoveries of my own.
* **Discuss possible legal issues\*\*. ->** This does not apply in my project.
* **Report your findings to the outside world in a decent way ->** I consider my portfolio, the research report and the powerpoint presentation my findings report.
* **Prepare for the presentation and demonstration to your classmates and write the research report. ->** Aside from the research report, I have also prepared a powerpoint presentation.
* **Conclusions**

This project was quite a challenge, representing the first interaction with hardware, even before the first workshops about that. As a consequence, research took more time than planned. Choosing a different device midway through the available time slot was also a setback. However, the main conclusion is that it is scary how easy it is to hack into devices and how important security measures are.

* **Resources**
* [**https://drfone.wondershare.com/unlock/hack-samsung-galaxy-s3.html**](https://drfone.wondershare.com/unlock/hack-samsung-galaxy-s3.html)
* [**http://forhackersonly.blogspot.com/p/how-to-hack-b.html**](http://forhackersonly.blogspot.com/p/how-to-hack-b.html)
* [**https://spyic.com/phone-hack/how-to-hack-a-samsung-phone/**](https://spyic.com/phone-hack/how-to-hack-a-samsung-phone/)