|  |  |
| --- | --- |
| Plan of Action  Honeyjar and Malware studies | Abstract  This document describes the background of this project, as well as being a clear summary of expected actions and responsibilities for all project members involved. |

# Version management

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Author** | **Date** | **Comments** |
| 0.1 | Morcel | 20-02-2018 | Added chapters |
| 0.2 | Alexander | 21-02-2018 | Added front page, as well as further defining of the problem definition |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Background 5](#_Toc506971345)

[2. Subject of research 6](#_Toc506971346)

[3. Goal and Problem Definition 7](#_Toc506971347)

[3.1. Problem definition 7](#_Toc506971348)

[3.2. Goal 7](#_Toc506971349)

[3.3. End-results 7](#_Toc506971350)

[4. Theoretical framework 8](#_Toc506971351)

[5. Tools of Research 9](#_Toc506971352)

[6. Organization 10](#_Toc506971353)

[7. Planning 11](#_Toc506971354)

[8. Costs 12](#_Toc506971355)

[9. Feasibility and risks 13](#_Toc506971356)

# Background

The current project group consists of nine people coming from four different universities.

|  |  |
| --- | --- |
| University | Project member(s) |
| Saxion (NL) | Alexander Pluimers  Morcel el Ouahbi |
| AAU (DK) | Jacob Veljin Jensen  Daniel Britze  Magnus Stensli  Robert Nielsen  Peter Moller |
| AGU (TR) | Ahmet Turkmen |
| UTP (PL) | Anna Switala |

Everyone except for the people from AAU are new to this project. These project members from AAU have worked on this project half a year prior to the rest and have made a base code.

Their assignment was to improve cybersecurity. They took their research to Android phones since according to their research, people store a lot of sensitive data on their smartphones and cybersecurity on smartphones isn’t deemed urgent by the masses at this point in time.

Saxion has brought two business IT students to the project. Their job is to create a system that is appealing for businesses. How do we sell this product? NOT FINISHED

# Problem Definition

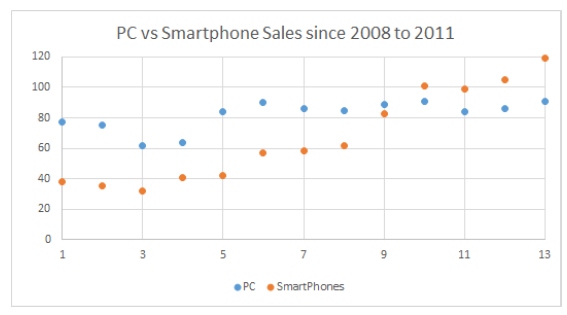
In this paragraph the group will describe what the reason for the project is as well as the desired end result when the project is finished. We will do this with the help of research questions. These questions will help us divide the project into smaller chunks. When all the subquestions have been answered you automatically answered the main issue.

## Statistics

Companies as well as regular consumers have a lot of sensitive data stored on their smartphones, for example (but not limited to):

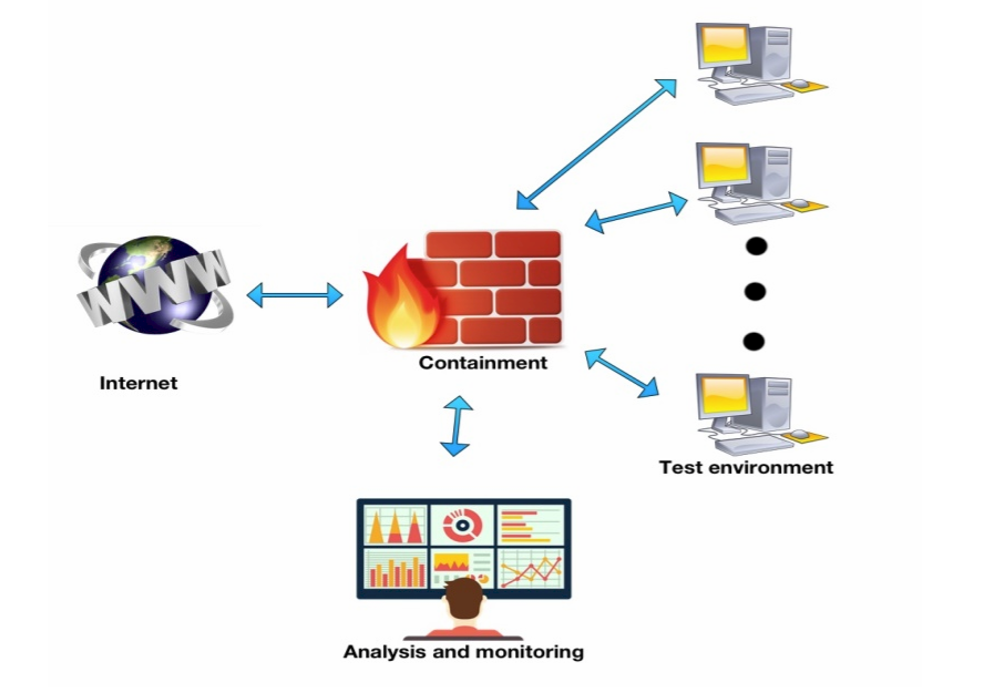
* Credit card data
* Compromising photos
* Passwords
* E-mails
* Customer data

This in itself is worrisome, however the popularity of smartphones is rising as well. At this point in time smartphones outsell PC’s. Computers have been susceptible to malware since they were first introduced to the market, however it seems that Android phones, while vastly gaining popularity over PC’s, are still relatively under protected to Malware attacks. This is represented in the graph below, which is derived from a survey done by the project members from AAU. (BRON HIERR)



To exploit the fact that the market hasn’t really focused on security on Android phones yet, the project members from AAU created a basic Honeypot system.

A Honeypot, as to be derived from its name, is a virtual machine that emulates a system, in our case an Android Phone, presenting it in such a way that it becomes interesting for malware to attack. This Honeypot system in its current state is still very basic and needs improving.

AAU has created a figure of how the honeypot system should work, this is illustrated in the following figure.

The three computers in the example will be running an emulated version of Android, making the emulation seem as realistic as possible, i.e. emulating human behavior. Once these systems are infected through the internet, the malware will be contained, and analyzed to determine what the category of the Malware is.

## 3.2. Goal

The goal of this Honeyjar is to provide intelligence on the nature of the Malware that is captured and contained in the quarantine. Furthermore, based on the intelligence that is gained in containment, the Honeyjar algorithm has to show improvement in recognizing Malware.

## 3.3. End results

At the end of this project the following will be finished and accomplished:

1. A functional Honeyjar system that shows improvement in recognizing Malware through Machine Learning
2. A Business Plan to describe the Business aspects of the Honeyjar and how to make the system profitable
3. At least 1 Android Virtual Machine that functions as bait for Malware

# Theoretical framework

# Tools of Research

# Organization

# Costs

# Feasability and risks

## Feasability

Feasability describes what the project needs to function, i.e. money, infrastructure, materials, expertise, and time.

### Money

For this project money is not an issue as all intercultural meetings are accounted for by EPIC.

### Infrastructure

One of the pillars of this project is that it’s intercultural, so project members will work together from their home countries. There are weekly online meetings where progress is discussed. Other than that there are plans to meet in a city somewhere in Europe at least one more time during the project.

### Materials

For setting up the server on which the Honeyjar is hosted, the University of Aalborg provides free server space. Other than that all project members will be using software that is either freeware or accounted for through a student license.

### Expertise

As the project group consists of 9 members, there are a different expertises; business, networking, and programming. These different expertises are useful for providing different approaches to the project.

### Time

All project members are expected to work on the project every day, ranging from a few hours every day to full-time. Even though the project group is the largest among the EPIC groups, the project is big and ambitious, so maximal effort is required.

## Risks

### Different deadlines

As all project members work on this project in a different year and/or in a different format (i.e. the Business project members are doing this project for their Minor studies, while the Danish group is doing this for their first year of school), the deadlines for each project member differ. This opens up the possibility that project members are going to follow their own agenda as opposed to working towards a common deadline as a team. To prevent this, the group created a planning with each deadline carefully noted.

### Miscommunication

Due to the intercultural nature of this project, we expect there to be some miscommunication and cultural differences. We try to avoid this by setting up ground rules.

# Appendices

## Appendix I: Planning

