WhatsApp Database Encryption on Android and BlackBerry
Project Plan

D. Cortjens A. Spruyt F. Wieringa

16th of November, 2011

Contents

1 Document Information **2**
- 1.1 Description . . . 2
- 1.2 Version History . . . 2
- 1.3 Acceptance . . . 2

2 Project Description **3**
- 2.1 Introduction . . . 3
- 2.2 Problem . . . 3
  - 2.2.1 Main Question . . . 3
  - 2.2.2 Sub Questions . . . 3
- 2.3 Goal . . . 4
  - 2.3.1 What encryption is used for the WhatsApp databases? . . . 4
  - 2.3.2 How strong is this encryption? . . . 4
  - 2.3.3 How is the encryption key generated? . . . 4
  - 2.3.4 Where is the encryption key stored? . . . 4
  - 2.3.5 What are the differences between the Android, BlackBerry and iPhone operating systems regarding database encryption? . . . 4
  - 2.3.6 Is it possible to decrypt the WhatsApp database? . . . 4
- 2.4 Scope . . . 4

3 Project Scenarios **5**
- 3.1 What encryption is used for the WhatsApp databases? . . . 5
- 3.2 How strong is this encryption? . . . 5
- 3.3 How is the encryption key generated? . . . 5
- 3.4 Where is the encryption key stored? . . . 5

4 Project Planning **6**
- 4.1 Activities . . . 6
- 4.2 Milestones . . . 6
- 4.3 Global Overview . . . 7

5 Project Organisation **8**
- 5.1 Team . . . 8
- 5.2 Communication . . . 8
- 5.3 Information . . . 8

Chapter 1

Document Information

1.1 Description

This document describes the project planning for the WhatsApp Database Encryption on Android and BlackBerry project. This small project is part of the Security of Systems and Networks subject of the System and Network Engineering course.

1.2 Version History

Version	Date	Author	Comments	Status
0.3	16th of November, 2011	D. Cortjens A. Spruyt F. Wieringa	- corrected some English sentences throughout the document	draft
0.2	15th of November, 2011	D. Cortjens A. Spruyt	- added CrypTool to the first (3.1) and second (3.2) goal in Project Scenarios (3) - added literature research to activities (4.1) and global overview (4.3) in Project Planning (4) - added GIT reposity information to information (5.3) in Project Organisation (5) - corrected some English sentences throughout the document	draft
0.1	13th of November, 2011	D. Cortjens	first version of the Project Plan	draft

Table 1.1: Version Management

1.3 Acceptance

Name	Role	Date
J. van Ginkel	teacher	
A. van Inge	labteacher	

Table 1.2: Acceptance

Chapter 2

Project Description

2.1 Introduction

The last few years the number of mobile devices has grown enormously. Nearly everyone owns a mobile device like a phone or tablet. Mobile devices are now little computers with the power of a normal desktop or notebook computer. People do not need a desktop or notebook computer anymore, because they can do everything with their mobile device and store everything on them. They're used to browse the web, make appointments and communicate with other people. WhatsApp has become a very popular application for sending messages. It's a free application that sends messages through the data connection of the mobile device. It's one of the first applications people install on there mobile device. WhatsApp is cross platform with versions available for the Android, BlackBerry, iPhone and Symbian operating systems. In the world of Digital Forensics WhatsApp has become an important and useful source of information. WhatApp stores messages and everything that can be sent in these messages (audio, locations, pictures, video, etc.) in a SQLite database. The location of this database is primarily on the memory card in the phone but alson on the internal memory of the phone when there is no memory card present. Examining the database is the way to do this without having to use the phone it self.

2.2 Problem

WhatsApp has changed a lot over the last couple of months. They've encrypted the messages sent over the data connection and even encrypted the databases stored on the memory card or internal memory. This has made it very difficult for Computer Crime Experts to search for the, in many cases important, communication between people. The Digital Forensics world is in need of decryption these databases, so this information can be used in the fight against crime.

2.2.1 Main Question

Is it possible to decrypt the WhatsApp database?

2.2.2 Sub Questions

The central question is answered through the following subquestions:

1. *What encryption is used for the WhatsApp databases?*
2. *How strong is this encryption?*
3. *How is the encryption key generated?*
4. *Where is the encryption key stored?*
5. *What are the differences between the Android, BlackBerry and iPhone operating system regarding database encryption?*

2.3 Goal

2.3.1 What encryption is used for the WhatsApp databases?

Determine which encryption cipher is used for the database on the Android, BlackBerry and iPhone operating system in the first week of the project.

2.3.2 How strong is this encryption?

Determine how strong the encryption is on the Android, BlackBerry and iPhone operating system in the first week of the project.

2.3.3 How is the encryption key generated?

Determine how the encryption key is generated on the Android (and BlackBerry) operating system in the second and third week of the project.

2.3.4 Where is the encryption key stored?

Determine where the encryption key is stored on the Android (and BlackBerry) operating system in the second and third week of the project.

2.3.5 What are the differences between the Android, BlackBerry and iPhone operating systems regarding database encryption?

Summarize the differences between the Android (and BlackBerry) operating system in the Project Report in the fourth week of the project.

2.3.6 Is it possible to decrypt the WhatsApp database?

Determine whether or not the WhatsApp database can be decrypted and write the conclusion in the Project Report in the fourth week of the project.

2.4 Scope

The project has the following scope:

- The global information from goal one and two in section 2.3 is collected for the Android, BlackBerry and iPhone operating systems
- The detailed information from goal three and four in section 2.3 is collected for the Android operating system
- The detailed information for the BlackBerry operating system is collected when this is finished or isn't possible for the Android operating system
- The solution for decrypting the database has to work on an unrooted mobile phone from a physical dump
- The solution for decrypting the database may work on a rooted mobile phone when this isn't possble for an unrooted mobile phone

Chapter 3

Project Scenarios

The following scenarios are presented with which to reach the goals presented in section 2.3 of chapter 2:

3.1 What encryption is used for the WhatsApp databases?

- Using CrypTool on the databases from the physical dump
- Using Nevis on the databases from the physical dump

3.2 How strong is this encryption?

- Compressing the databases from the physical dump and looking at the compression percentage (to determine the entropy)
- Using CrypTool on the databases from the physical dump (to determine the entropy)

3.3 How is the encryption key generated?

- Interchanging the micro Secure Digital memory card with the database from one mobile phone with the other
- Copying the database from one mobile phone to the other
- Using an older database (backup) by deleting the current one
- Erasing the mobile phone and then use the former database
- Running plain attacks on the encryption
- Debugging code
- Reverse engineering code

3.4 Where is the encryption key stored?

- Debugging code
- Reverse engineering code

Chapter 4

Project Planning

4.1 Activities

The project has the following activities:

1. writing Project Plan
2. literature research
3. applying WhatsApp data Android
4. applying WhatsApp data BlackBerry
5. applying WhatsApp data iPhone
6. creating physical dump Android
7. creating physical dump BlackBerry
8. creating physical dump iPhone
9. determing encryption Android
10. determing encryption BlackBerry
11. determing encryption iPhone
12. determing encryption strength Android
13. determing encryption strength BlackBerry
14. determing encryption strength iPhone
15. determing encryption key generation Android
16. determing encryption key generation BlackBerry[1]
17. determing encryption key storage Android
18. determing encryption key storage BlackBerry[1]
19. writing Project Report

4.2 Milestones

The project has the following milestones:

1. Project Plan is approved
2. global information collected
3. detailed information Android collected
4. detailed information BlackBerry collected[2]
5. Project Report is writen

[1] activity is done when this is finished or isn't possible for the Android operating system
[2] milestone is reached when this is finished or isn't possible for the Android operating system

4.3 Global Overview

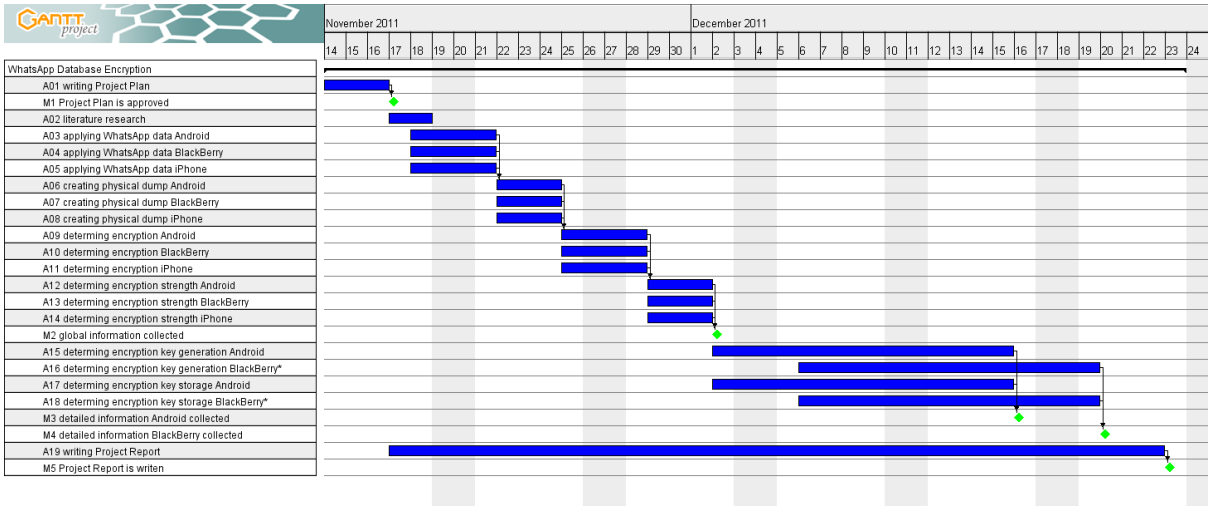

Figure 4.1: Gantt Chart

Chapter 5

Project Organisation

5.1 Team

Name	Role	Skills
D. Cortjens	student	Forensics and Programming (intermediate)
A. Spruyt	student	Programming (advanced)
F. Wieringa	student	Programming (basic)

Table 5.1: Team

5.2 Communication

The communication is conducted through scheduled meetings and email. There will be meetings twice a week on monday and thursday after the lectures.

5.3 Information

The project documents, files and software will be held in a GIT repository. The GIT repository is stored on the server *oslo.studlab.os3.nl* and has a specific folder stucture as shown in table 5.2. Large files such as physical dumps will be transfered by external hard drive.

Folder	Subfolders	Description
documents	-	The folder with all the documents created and used within the project.
	literature	The subfolder with all the literature used within the project.
	project_plan	The subfolder with all the source files for the Project Plan.
	project_report	The subfolder with all the source files for the Project Report.
files	-	The folder with all the other files used within the project.
software	-	The folder with all the software used within the project.

Table 5.2: Folder structure