Table of Contents

Chapter 1

Chapter Heading

1.1 Section Heading

1.1.1 SubSection Heading

SubSubSection Heading

Paragraph Heading with some text after

- Itemize

- One

- Two

1. Enumerate

2. One

3. Two

Description Description

One First

Two Second

Table	Headers	here
Lots of	rows	go here
Right Aligned	Left aligned	Centered

Table	Paragraph
Small header	lots of writing that can turn into a paragraph and will take up all of the remaining space in the page.
This	Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

[?]
[?]
[?]
[?]
[?]

This is a sentence in green
This is in red
This should be blue.

'\\' above means `newline`. Repeated white space is always treated as a single whitespace—space, tab, newline.

Paragraphs are separated by a blank line.

- `Typewritter font`

- *Emphasised is better than bold/italics with* emph *inside*

- **Bold font with *emph inside***

```
public void javaMethod() {
   doSomething();
   if (happy) {
      clap(hands);
   }
   return new String("Really want to show it.");
}
```

Listing 1.1: This is the caption

Chapter 2

Introduction

2.1 Motivation

As the popularity of mobile devices increases, there is an increasing tendency to use these as a convenient means of reviewing and revising documents on-the-move. Where these documents are of a confidential nature, particular attention must be paid to the fact that mobile devices are much more subject to compromise that traditional desktops, which are usually more extensively protected by the security measures implemented as part of an organisation's internal network.

One solution to this is the storing of documents in encrypted format. However, where there is a requirement for collaborative working across more than one organisation, this introduces the additional problem of group key control and distribution in order to mediate access to the documents in question.

2.2 Aims and Objectives

- The primary objective of this project was to implement a scheme for the secure sharing of confidential documents within the context of a mobile device which is running the Android operating system.

- The intention is to produce a prototype android app which will serve as a platform to implement and evaluate the various security features. As such, it is anticipated that the app may appear somewhat utilitarian; any additional capacity within the development phase will be channelled into improving functionality and enhancing cryptographic security mechanisms rather than developing a sophisticated graphical user interface.

2.3 Scope

Shared files are held on a secure web server. Since the web server is not part of the trusted group, it should hold no unencrypted files and no ability to perform

4

decryption.

Any database used for performing user authentication, etc. is deemed to be secure.

Any attacker inserting malware onto the mobile device may be able to access files stored on that device but would not be able to access that data whilst held in the device memory.

The requirement to maintain security of documents at all times is such that the processing overhead associated with key management and encryption/decryption is deemed acceptable.

For the purposes of this application, it is not necessary to consider performance and battery usage issues associated with the use of the mobile device, as it is deemed that the application will be run relatively infrequently.

Limitations

In order to protect from active attackers, the initial intention is to ensure that documents are not saved to disk in unencrypted format - an unencrypted document will be held in memory and a simple rich text editor will be implemented within the application to allow reading and editing. It is acknowledged that a fully developed app would need to provide integration with existing 3rd-party document-handling applications. This would require further work and also involve use of secure hardware to ensure that security is maintained at all stages. Currently it is anticipated that such features will be beyond the scope of this project.

It is anticipated that, in a fully-developed system, initial creation of documents would take place in a desktop environment; therefore, implementation of a suitable desktop client is outside the scope of this application.

2.4   Overview of Report

Chapter 3

Background

Chapter 4

Analysis and Specification

Chapter 5

Solution Design

Chapter 6

Implementation

Chapter 7

Evaluation