Confidential Document Sharing System for Android Devices - Project Proposal

Julie Sewards

23rd June 2014

1 Introduction

As the popularity of mobile devices increases, there is an increasing tendancy 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 Project objectives

The primary objective of this project is 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 functiality and enhancing cryptographic security mechanisms rather than developing a sophisticated graphical user interface.

3 Deliverables

The project deliverables will be:

- a dissertation document detailing the design and implementation of the application and a discussion of the key features of the security protocols used.
- an android app for reading and performing basic editing of secure documents using an appropriate user authentication and key management mechanism.
- a central repository for shared documents (probably implemented as a web server).

4 Initial Assumptions

- 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 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.

5 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.

6 Timescales

Item	Activity	Targeted Completion Date
1	Initial familiarisation with material and completion of project proposal	20/6/14
2	Setup of development environment	27/6/14
3	Familiarisation with technologies, including android framework, web server and basic PHP, java security API	2/7/14
4	Production of initial prototype implementing basic app and file transfer mechanisms but without encryption	7/7/14
5	Research and evaluation of appropriate group key distribution schemes	12/7/14
6	First implementation with security features added	14/7/14
7	Complete Introduction and related work write up	25/7/14
8	Final implementation with basic security features	30/7/14
9	Review of progress and identification of additional features for development	6/8/14
10	Finalise software	15/8/14
11	Complete first draft of report	18/8/14
12	Complete final report	29/8/14