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.

[4]
[2]
[6]
[5]
[3]

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 communications devices increases, there is a growing 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 more vulnerable to compromise than traditional desktops, which are usually more extensively protected by the security measures implemented as part of an organization's internal network.

There are multiple mechanisms for keeping files secure on company servers whilst allowing employees the necessary permissions to work collaboratively with sensitive data as required. As the mobile device culture becomes more prevalent in the workplace, the addition of Mobile Device Management (MDM) applications empowers users to also access corporate data via their mobile devices whilst still allowing IT departments to retain a degree of control over data security.

Thus, it is acknowledged that maintaining the security of confidential documents can be challenging, even with the weight of a corporate IT infrastructure behind it. In this project, we seek to address the issue of allowing groups of users from different organizations (i.e. with no shared IT infrastructure) to collaborate securely on confidential documents and furthermore, to access these documents via a smartphone or tablet computer whilst minimizing the risk of exposing sensitive information to a potential attacker.

2.2 Project Aims

The primary aim of this project was to implement a scheme to facilitate secure sharing of confidential documents between a number of collaborators (typically less than 15), subject to the following constraints:-

- Groups are self-organizing and represent multiple organizations, hence they cannot draw on the support of any central IT services.

- The documents involved are confidential in nature and hence should be encrypted both in transit and at rest.
- Group members wish to be able to access documents on a mobile device which is running the Android operating system.
- The solution devised should use only well-tested cryptographic techniques and standard libraries and should minimize the amount of trust to be placed in a third-party.

In pursuit of these aims we developed a solution called Securely Share, consisting of a detailed design of the security components of the system and a prototype android application (SecurelyShare) to provide a platform on which to implement and evaluate the various security features. It was acknowledged that, in a live setting, documents would usually originate on a PC rather than on a tablet device and thus the system would also need to a PC-based component. However, within the time constraints of the project it was considered infeasible to develop a fully featured system; our solution is submitted rather as a 'proof of concept'.

2.3 Overview of Report

The subsequent chapters of this report will deal with the design, implementation and evaluation of the project. Chapter 3 introduces some of the background material on key technologies used and presents an overview of the android applications reviewed as part of our preliminary research. In the light of this research, Chapter 4 presents a detailed analysis of the problem and expands the aims outlined in TODO into a more complete project specification, including details of the threat model against which we are attempting to defend. Chapters 5 and 6 deal with the solution design and implementation Need detail of rest of chapters here

Chapter 3

Background Material

In this chapter we will introduce some key aspects of the android architecture and its security features. We will also examine the features offered by the Dropbox API and finally we will look briefly at some of the commercial applications which were reviewed as part of our initial research and which offer some features similar to Securely Share.

3.1 Android Security Features

Android provides an open source platform and application environment for mobile devices. It has a layer based architecture whose foundational component is the Android Operating System. Based on the tried and tested Linux 2.6 kernel and modified by Google to include some additional features, it is the comprehensive user permissions model inherent in Linux that is responsible for providing the separation between applications that is a key feature of Android security. At installation time, each application is assigned a unique user ID (UID);at runtime each application is run as a separate process an as a separate user with its given UID. This create an Application Sandbox, protecting any resources belonging to that application (memory space, files, etc.) from being accessed by another application unless specifically permitted to do so by the developer.

Cryptography Android provides a set of cryptographic APIs for use by applications.

3.1.1 Android Components

3.1.2 Android Permissions

ANDROID COMPONENTS ANDROID PERMISSIONS

3.2 Dropbox API

Dropbox is a cloud storage service that also offers users automatic backup facilities, file synchronization across devices, and the ability to share files with other users. It provides multi-platform client applications plus a series of public APIs that enable different subsets of the Dropbox functionality to be integrated into third-party applications.

On the Android platform, Dropbox offers three APIs, described on its website as follows:-:

Core The Core API includes the most comprehensive functionality including features such as search, file restore, etc. Although more complex than either of the other two to implement, it is often more suitable when developing server-based apps.

Datastore The Datastore API provides a means of storing and synchronizing structured data like contacts, to-do items, and game states across all the user's devices.

Sync The Sync API provides a file system for accessing and writing files to the user's Dropbox. The Sync API manages the process of synchronizing file changes to Dropbox and can also provide the app with notification when changes are made to files stored on the server.

For the purposes of the SecurelyShare app, although it offers the most basic interface to the Dropbox server, the Sync API was deemed to support both the functionality required for the prototype and some additional facilities which could be implemented at a later date in order to improve the overall user experience.

Each app on the Dropbox Platform needs to be registered in the App Console and the developer needs to select which permissions the app requires. These permissions determine the type of data that the app can access in the user's Dropbox. For the Sync API, three levels of permission were applicable:

- App folder: this creates a folder in the user's Dropbox with the same name as the app, all files relating to the app are kept here and access is restricted to this folder and its subfolders.
- File type: the app is given access to the user's entire Dropbox but is restricted only to seeing files of certain types (documents, images, ebooks, etc.)
- Full Dropbox: the app is given unrestricted access to the user's Dropbox

TPM?

3.3 Review of Similar Applications

One of the security claims of cloud storage provider, Dropbox, is that user data stored on their servers is fragmented and encrypted using 256-bit AES. However, although users may feel reassured by these claims, it is also to be noted that

since this encryption is applied server-side, the servers also have access to the keys required to decrypt this information. Furthermore, the Dropbox privacy policy states that,

> "We may disclose your information to third parties if we determine that such disclosure is reasonably necessary to (a) comply with the law; (b) protect any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or our users; or (d) protect Dropbox's property rights.

It may therefore come as little surprise that there are an increasing number of client-side encryption applications available that integrate with Dropbox and other similar cloud services to ensure that, even if files are disclosed, the organisations concerned would have no access to decryption keys.

Although there are a significant number of encryption applications available, our research was not able to identify any robust security comparison of the various products on offer. We decided to consider two commercially produced applications, Boxcryptor and SafeMonk

When trying to evaluate these products there appeared to be a paucity of robust reviews from respected members of the security fraternity and many of the review that were available seemed to focus more on the usability of applications rather than on their security features. One of the only ways that a security application can truly be evaluated is if the source code is available for community scrutiny as security flaws often fail to come to light just from using the product. Most of the products we looked at seemed to be designed primarily for personal file protect - some professed to offer sharing although some of the less polished versions required manual sharing of encryption keys. Some of them were unforthcoming about exactly how they work

Two products that we examined in greater details, partly because they seemedto be higher profile products although that may simply be due to the fact that they were commercial products with a paid version as well as the free version that we tested and hence had larger marketing budgets. It may also be because they had more security credibility however there was a common trend among the examined applications to use AES for encryption of the actual files themselves and some implementation of RSA to manage the key exchange, In all the cases that we examined there was a central server that was used for key management, although both Boxcryptor and Safemonk were keen to strees that they were "tapproof" or "zero-knowledge" servers and had no access to key material that would enable them to decrypt user files. There justification for storing the user's private key on the server was that it would allow the user to install the application on multiple devices and they both used password-based encryption (PBE) in order to secure the key on the server. Although the servers use key-stretching algorithms to derive the encryption keys, we should always be aware that users can be very poor at choosing strong passwords and at keeping them secure. (In a study of password reuse, Bonneau [1] observed that 43 percent of users reused a password across multiple sites)

"http://source.android.com/devices/tech/security/system-and-kernel-level-security"

”http://link.springer.com/book/10.1007/978-1-4302-4063-1page-1”

Chapter 4

Analysis and Specification

Key generation and sharing currently done from PC rather than android device Folder management and sharing done outside of app - could be added but may require switching to a more complex dropbox api. Cost-benefit analysis

Early design considerations • who generates keys • how are keys generated • how are keys distributed • issue with public key - how would we stop Mallory uploading bogus documents • issue with where to place trust • how to manage letting decryption know group - flirted with shared preferences Issue: if generate [rivate key on device, it is device specific - ability to import would allow same keystores to be used on multiple devices for4 same user • decision to ignore considerations like battery life and User authentication and need to block after failed attempts • large files • network connectivity • battery life • small memory • multithreading for gui • where to encrypt • model to use for file distribution and storage Means of distributing certificates is outside of scope - as these are public, any means will do.

Chapter 5

Solution Design

Reasons why didn't choose ID based cryptography or password based solution - aim is to use simplest solution that works

Design. A high-level account of the structure of your software and how it works. What algorithms does it use? How do these compare with alternatives? What were the main design decisions you took, and their justifications?

Althou prototype allows for encryption of files stored on the device, in practice the very fact that there are files on the device that the user wants to encrypt violates our central tenet that plaintext should never be stored to disc.

Chapter 6

Implementation

Implementation and testing. A detailed account of the implementation and testing of your software. Explain what data structures you used, and how the algorithms were implemented. What implementation decisions did you take, and why? There is no need to list every little function and procedure and explain its working in elaborate detail; use your judgement on what is appropriate to include. use of .xps, .xeb For improvement, use custom file extension registered with Dropbox then would only ever see encrypted files use of bundle for passing data between activities use of interface for passing data back from dialog Performance problem - introduced buffering Splash screen and initialization didn't use onStoreState etc. - didn't worry about restoring exact user position as prototype and system stores GUI stuff Use of singleton Keystores moved to external storage for testing and demonstration purposes. In a production app, these should be moved back to internal storage in order to take advantage of the additional protection afforded by android's inbuilt security mechanisms Removal of keystores upon 3 successive failed password attempts – al present it just shows a message saying that the keystores have been deleted but doesn't actually remove them from the device. In a live system this would need to be implemented. • use of xml rather than java for managing onClick - why was this done and when is it not applicable Major issues with keystore, certificates and default providers. Challenge of absence of built in file manager DROPBOX ISSUES • dbx stuff does not implement serialisable or parcelable • Dropbox synchronization issues - developed everything using App specific access then discovered that this doesn't allow any use of shared folders so had to redesign Challenge of unavailability of BKS on pcs in school No access to key tool in android Include information about algorithms and key lengths Fragments TESTING Testing - it is ok to say that I tested by inspection Explain why unit testing is not meaningful

Issue: if generate [private key on device, it is device specific - ability to import would allow same keystores to be used on multiple devices for4 same user

Assumption that encrypted blobs are probably also created on PC - simple PC version of program developed to address this, although no gui developed

Chapter 7

Evaluation

ACHIEVEMENTS • What works well EXPLAIN HOW WELL SOLUTION MEETS OBJECTIVES - WHAT YOU HAVE LEARNED - WHY ANDROID DEVELOPMENT WAS A CHALLENGE major challenge of the fact that android is an operating system not a programming language - event driven programming FURTHER WORK • From prototype to production - next steps Write as though you are porviding a basisi for a good cs graduate to continue the work - assume they have already done some android development SECURITY EVALUATION Did not implement signing in prototype as largely meaningless with self-signed certificates. Purchase of appropriate certificates for authentication of signatures would be required for a complete solution Attacks and issues to consider • anonymity • forward secrecy • revokation • man-in-middle Delete keys after failed password attempts Write about how p[rotocols as as important as implementation - need to support this view from academic papers Talk about why it doesn't matter that encrypted copies of group key are available on dropbox nelenkov.blogspot.co.uk - credential storage enhancements in Android 4.3 out of bounds channel - side channel attack Write about issues to do with public key distribution and the need for signing Talk about decision not to implemenmt passing decrypted data directly to another app without needing to write to external storage Don't zero out passwords after use No implementation of digital signatures so vulnerable to man-in-middle Decision to use same password for keystore and aliases - trade off of added security against temptation for users to use insecure passwords or write them down

Group needs admin, although any group member can serve in this role. It is also possible to delegate this to an administrator who is not part of the group without giving them access to the group encryption key. However, if the admin was corrupt, the fact that they had access to the private key for signing the encrypted group key would still be a problem.. Useful phrase "a more sophisticated attacker"

Threats: • Malware on device • Attacker snooping around external storage but not one with root access • Lost device with app open (minimal protection) but can unlink from dropbox remotely so would only have a very small window of opportunity to decrypt files currently stored on devicewhilst keystore is unlocked • Could have had different password for each group • Could make user re-enter

password for each file – trade off between added security in event of lost device and templtation for user to choose a weaker password

Maybe argue why solution is secure here PROTOTYPE EVALUATION dependent on exactly correct alias for groupid and folder name • Is designed as a "proof of concept" • Aspires to use "best practice" within the code • Uses well-tested cryptographic techniques and standard libraries • Adheres to the stated security requirements No ability to change passwords etc added at present

EVALUATION OF PERSONAL LEARNING • zero knowledge starting point • Android is a whole new operating system not just 'Java with extra bits' • Unfamiliar API's operating in a sub-optimal environment

Bibliography

[1] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The tangled web of password reuse. In *Proceedings of NDSS*, 2014.

[2] Nicholas Fang, Hyesog Lee, Cheng Sun, and Xiang Zhang. Sub–diffraction-limited optical imaging with a silver superlens. *Science*, 308(5721):534–537, 2005.

[3] Dylan M Owen, Carles Rentero, Jérémie Rossy, Astrid Magenau, David Williamson, Macarena Rodriguez, and Katharina Gaus. PALM imaging and cluster analysis of protein heterogeneity at the cell surface. *Journal of biophotonics*, 3(7):446–454, 2010.

[4] WS Rasband. ImageJ, US National Institutes of Health. *Bethesda, Maryland, USA*, 2012, 1997.

[5] Michael J Rust, Mark Bates, and Xiaowei Zhuang. Sub-diffraction-limit imaging by stochastic optical reconstruction microscopy (STORM). *Nature methods*, 3(10):793–796, 2006.

[6] David J Williamson, Dylan M Owen, Jérémie Rossy, Astrid Magenau, Matthias Wehrmann, J Justin Gooding, and Katharina Gaus. Pre-existing clusters of the adaptor lat do not participate in early t cell signaling events. *Nature immunology*, 12(7):655–662, 2011.