Project Research Document – Secure SMS

X00093748 – Gary Morgan

3rd October 2014

Detailed Discussion

For my project I’ve chosen to do a secure SMS service for use on a Windows Phone. The application will allow users to send messages over mobile networks to other users. In order to ensure privacy from eavesdroppers the application will use decryption and encryption. I would like to also be able to use signed messages in order to deter both passive and active attackers from seeing the plaintext of each message.

Nowadays there are many SMS services for use as an app. Yet some people who are using these apps would be sending sensitive information and as these apps don’t contain any security a network operator or even any eavesdropper will be able to see messages shared between two users. This is where secure SMS comes in as it can use encryption and a private key to ensure privacy between parties.

Each user will have their own profile, using their phone number as an ID to access the app. They will also be able to set a username for display purposes. I hope to have a lot of extra functionality such as creating group chats in which multiple contacts can speak or being able to send multimedia messages.

A password will be shared between both sender and receiver that is unique to them only. The sender will send a message and set a password. The receiver will receive an encrypted message and will be able to decrypt it using the shared password in order to get the original message in plaintext.

Privacy is becoming a very much talked about topic recently which is why I believe the user base for this app will grow in the coming years. With many big companies like Facebook being accused of having zero privacy in their messenger applications and many people worrying about who can see their messages or are they safe from eavesdroppers and hackers.

Other possible features could be video sending, or if possible I would like to include encrypted calls or video calls. However this is only a possibility should I get the time to include or if it is even possible with the tools I have.

Existing Applications in this Domain

There are a few different secure SMS apps on the Windows Phone Store. These can be split into two types. The high levelled apps created by companies or teams of developers and the low-level ones created by single developers. Here are some examples of high-level apps.

|  |  |  |
| --- | --- | --- |
| Name | Similarities | Differences |
| BlackBerry Messenger | Uses AES encryption  Sends secure messages through encryption and decryption | Broader compatibility than most apps  Businesses can obtain a unique encryption key  Unique PIN |
| TextSecure | Sends secure messages through encryption and decryption | Uses standard text messages rather than the application  But less secure |
| Gliph | Sends secure messages through encryption and decryption  Pseudonyms | Cross-platform. Has a desktop service as well.  Can permanently delete any trace of a message |
| Wickr | Group messaging  Sends secure messages through encryption and decryption | Allows expiration date for messages  Removal of metadata |
| Telegram | Sends secure messages through encryption and decryption  Group chats | Message stored in cloud  Windows Phone support |

Platform, Technologies and Libraries

For my application I will be using Microsoft Visual Studio with C#. I picked C# over Java as it is my preferred language personally and also I believe it offers more features that will contribute towards the application. I like to use the code analyser included with Visual Studio as It is a very handy addition and Visual Studio runs brilliantly.

Visual Studio 2013 is the ideal platform for developing with the Windows Phone as it has great Windows Phone emulators that run inside it.

The app will be originally developed for Windows Phone 8 but I would like to add it to Android and possibly even iOS given the time.

I’ll use the C# library that is included in Visual Studio 2013.

As the application is an end-to-end messaging service that will use the users phone number as identification and the conversations will be saved to the phone I will not need to use a database or online storage.

The Risks

The app should be safe from risks involving storage due to saving on the user’s phone. However there are some possible risks that I may come across during development.

* The main risk would be being unable to get the encryption working on time. As the main component of the project without any encryption or decryption I won’t have a functional app.
* Depending on 1 library in Visual studio may be a problem. However I don’t see it causing any trouble.
* I am currently depending on an emulator for Windows Phone for testing. This may cause problems if there is any difference between the emulator and actual phone. However I plan on acquiring one soon.
* There is currently less support and other apps to research for the Windows Phone as opposed to other operating systems such as iOS and Android.