SECURE FILE TRANSFER APPLICATION

Final Report

Author: Aoife O'Brien

Student ID: C00214279

Project Supervisor: Patrick Tobin

Recipient: Institute of Technology Carlow

Date: Monday 20th April 2020

Abstract

This document consists of a reflection and discussion on my final year project. A number of aspects will be discussed such as elements that were and were not achieved, learning outcomes, problems encountered and how they were overcome, and what I would do differently if starting over again. Also covered in this document are the module descriptions, reporting of how some elements changed from the initial plan and design, along with the testing that was performed to ensure reliability of my product. This report has been written in relation to the secure file transfer application outlined in the previous documentation, as part of a fourth-year module of the Cybercrime and IT Security course in I.T. Carlow.

Contents

Introduction

This document will contain an overview of my experience of creating my final year project. It includes details on various aspects of the development process such as experience with new technologies, what I feel I could have improved on and how I might have made those improvements.

This document will be discussed under a number of headings; project description, learning outcomes and project review.

The learning outcomes will cover both the personal and technical learning outcomes. The project review section will contain information about the perceived success of the project with regards to what went right and wrong, along with what is still outstanding. Project review will also outline the aspects of the project that were achieved and those that were not, along with the deviation of the final application from the initial proposed application.

Project Description

Secure File Transfer Overview

Secure file transfer refers to the sharing of data via a secure and reliable channel. It is used to safeguard proprietary and personal data in transit and at rest.

Simply having the capacity to transfer a file from one location to another is not enough. Businesses today face more security threats than ever. They need a secure file transfer system in place to protect and reliably transfer their sensitive, business-critical data (globalscape.com 2020). Secure file transfer aims to increase security and compliance for individuals and businesses today.

Project Overview

This application consists of an interactive graphical user interface (GUI) which enables users to send and receive files securely over a network. Although the application is targeted at organisations, it is suitable for use by individuals in a home network also. This application will provide an easy-to-use and efficient system for users and will aid them in improving their security posture.

Architecture & Technologies

The application uses the following technologies:

- **Front-end:** Java
- **Database:** MySQL
- **Server:** Java sockets

Tools Used

- Eclipse IDE
- Java runtime environment
- MySQL Workbench
- Creately.com

Project Review

Problems Encountered

Too much time spent on the user interface design

Even though I had some previous experience with Java, I had not used the language in quite some time, and it took a while to get used to using the language again. To add to this, I had some issues with the toolkits that were used in the design, including elements not working when the application code was moved from one device to another. This meant that I had to redesign the UI from the start again multiple times. This led to me spending longer on the user interface that I had initially planned. I also found myself getting too bogged down with design of the user interface and because of this, functionality implementation started later than I had initially planned.

Time lost on components that were changed and removed

Due to design plans changing throughout the process in order to resolve certain issues or to improve the application, technologies used were changed, and elements were added and removed. For example, after feedback from my project presentation in January, compression of the files was implemented before encryption with the aim of increasing the speed of the application as well as allowing a variety of file types to be handled. However, problem arose when encryption was added into the application. This led to more research being carried out about compression and decompression of files in order to try and resolve the issue. During this research, I discovered that while file compression would help with speed, it actually weakens the security of the encrypted files. As security is a top priority in my project, I had to make the decision to remove the compression and decompression function, but unfortunately, this also meant that I had to reconfigure my encryption functions as the parameters had all changed. This led to a quite substantial loss of time, which also had a knock-on effect of delaying the later functionality being implemented and therefore, I did not get to complete all the modules and features that were initially planned due to time constraints.

More research required

Despite all the initial research that I performed, there is still a lot that I have to learn. This was evident throughout my project regarding encryption. After my initial research, I had decided on symmetric encryption along with a choice of encryption algorithms for the users. However, throughout the project, I discovered an encryption implementation called hybrid encryption. As discussed in the design manual, hybrid encryption is a combination of asymmetric and symmetric encryption in order to benefit from the strengths of both. If I had been aware of hybrid encryption before I started designing my application, it would have saved me significant time, instead of having to learn about it from scratch while also trying to implement it into my application. This caused a delay in the progression of the creation of the application. If I was doing this again, I would ensure that I was familiar with all my options of technologies before starting the development phase. I believe I could have done more research regarding some elements of my project.

What was Achieved

All core functionality for the application was achieved, including;

- User registration, authentication, session management and logout capabilities.
- User interface design and navigation development.
- The creation and configuration of MySQL database exists which holds the users' information and interacts with the application through an API.
- Sending and receiving functionality which allows for encrypted files to be sent and received between users of the application on the same network.
- Hybrid encryption and decryption of the data, using AES for the symmetric component and RSA for the asymmetric component.

What was not Achieved

The elements of the application that were not achieved include;

- VPN Tunnel:
  The initial plan for the application included the incorporation of a VPN tunnel into the transferring of the files with the intention of adding an extra layer of security. Unfortunately, time constraints did not allow for this to be implemented.

- Password Reset:
  Although a password reset link exists in the user interface, time did not allow for this functionality to be included as intended. This was because I gave preference to the more important components of the application once I realised that I would not get all functionality completed.

- Notification Message:
  The notification message that was to be displayed to the sender upon successful receiving of the file that they sent was not implemented due to time constraints. Once again, I gave preference to the main functional and security components of the application.

- Deployment:
  The application has not reached the phase of full deployment. The application currently resides on the development and testing devices only, but has been packaged into an executable jar file which launches and runs the application outside of the development environment. The application would require more work and configuration before it could be deployed to other machines and networks. For example, some hardcoded directory paths currently exist within the application. While I know that this is not best security practice, it was necessary in order to achieve all the functional requirements of the application in the time allowed. I would remove all hardcoded information and implement correct configuration if I had more time, and definitely before I would deploy the application.

What I would do differently if starting again

If I was starting again, I would do the following things differently;

Better Time Management

I would organise my time better if I was doing this project again. I would start the development phase earlier than I did this time. Although my project has all the core functionality included, it did suffer as a result of lost time and some incorrect time allowance for different aspects of the project, e.g. spending too much time on the user interface and changing between different encryption types.

I would also ensure that I allowed for time to implement the VPN tunnel for added security. I would have liked to do this because I think it would have been a positive challenge for me and I would have liked to put my theory knowledge of this technology to practical use. I also know it would have added more value to my project.

More Research

If doing this over again, I would perform more thorough research into the technologies and tools available to me, to help ensure that I make the best possible choices prior to the development phase, and therefore save time throughout the process to allow for more work to be achieved. I would also ensure that the technologies I choose are compatible with each other. I would try and plan better for potential problems that could arise throughout the process and the consequences that they could have on my project.

Differences from the initial design

During the year, the project evolved in various ways. These changes included;

Encryption and Decryption

The encryption and decryption algorithms and type used changed from the initial design. Instead of using symmetric encryption, a hybrid implementation was used instead for increased security and efficiency.

Server Choice

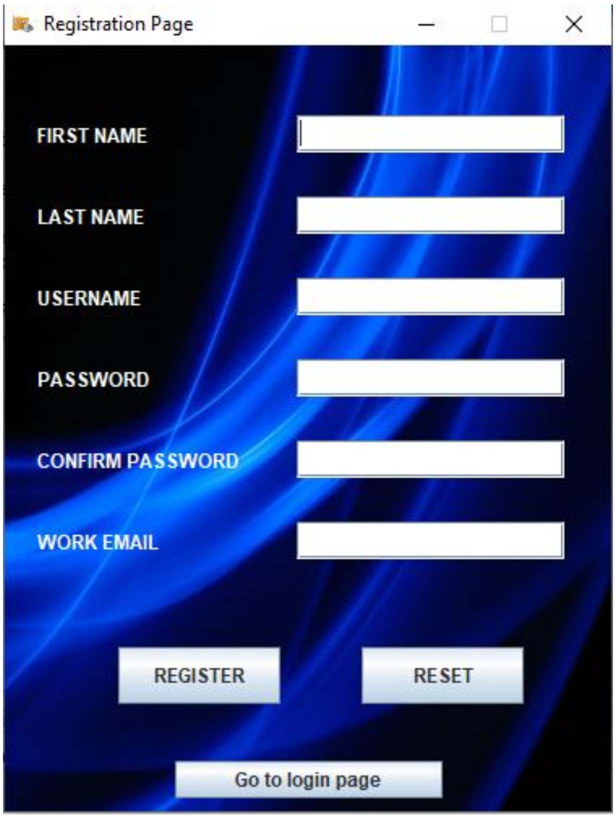
Prior to the development phase, the plan was to use an application server for the application. Throughout the development phase, it was decided that Java sockets would be used instead to allow for client/server communication regarding the transfer of files. The socket code is detailed in the accompanying technical manual.

Final Design

The finished application looks as follows;

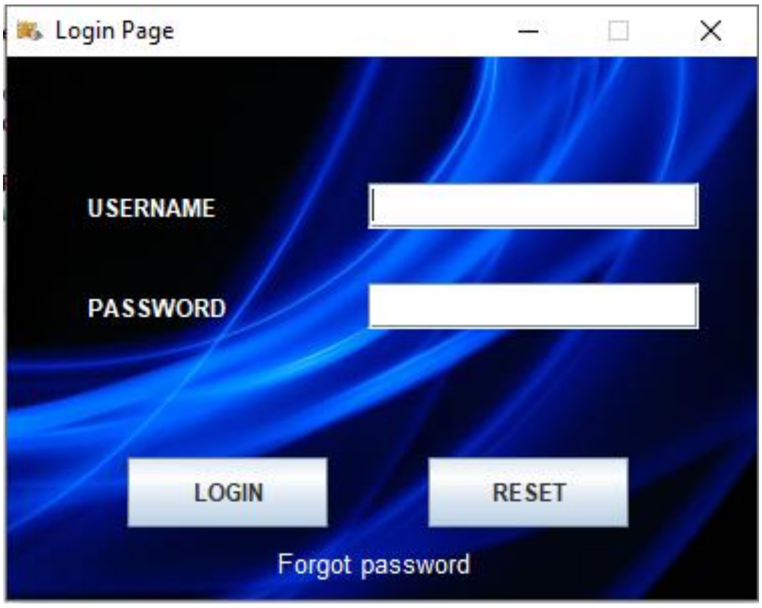
1. Registration Page

   Upon launching the application, users will see the registration page pictured below. Here, users will enter the information required and will become registered with the application. If a user is already registered, they can select the button at the bottom of the screen to go straight to the login page. A reset button is also provided in case a user enters incorrect credentials by mistake and wishes to start again. The reset button clears all the fields on the screen.



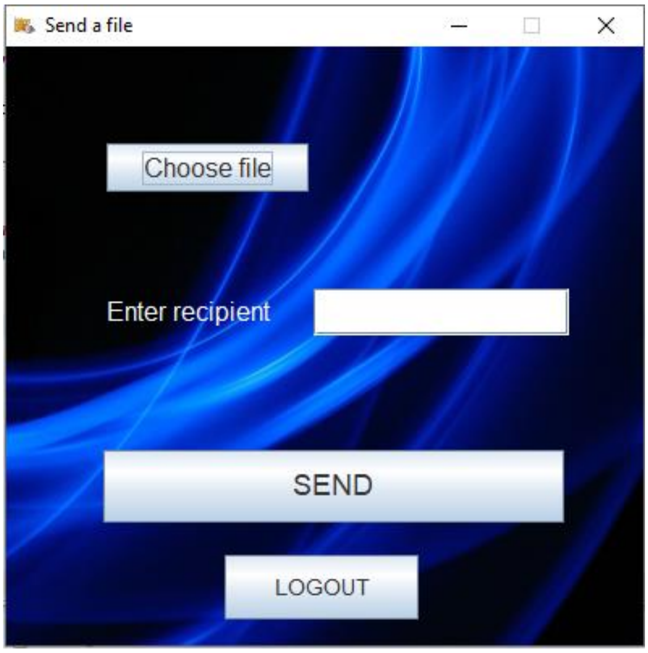
2. Login Page

The login page looks as below. Users will enter their username and password to login to the application. A reset button is also provided in case a user enters incorrect credentials by mistake and wishes to start again. The reset button clears all the fields on the screen. Users can also click the link provided at the bottom of the screen to reset their password if necessary.

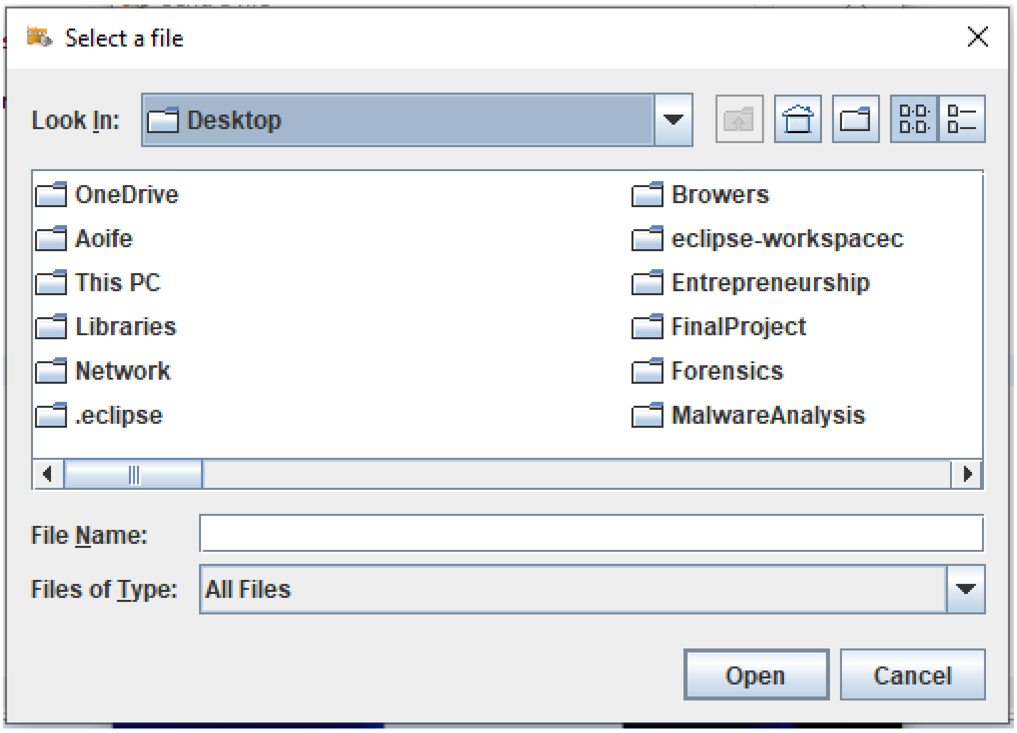


3. Home Page

   Upon users successfully logging in to the application, the home page will be automatically loaded, which will be where users send their files.

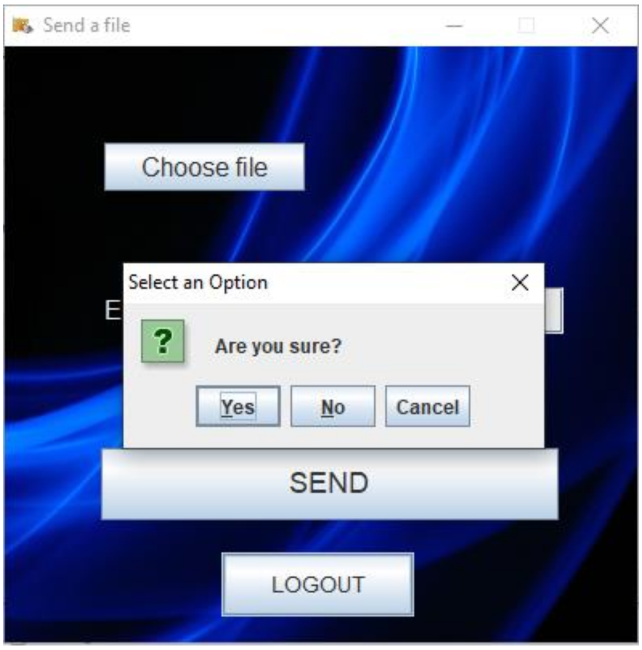


The choose file button will open a file chooser, allowing users to choose a file from their device to send using the application.



4. Logout Page

   Users can logout of the application using the button provided. A pop up box will appear on the screen asking the user to confirm or cancel the logout. If a user clicks the yes option, they will be logged out successfully. If a user clicks no, they will remain logged in to the application until the choose to logout.



Are you sure?

Testing

Testing was performed throughout each stage of the development process. This included checking each feature worked correctly before moving on to the next. This allowed me to identify errors, and make changes where necessary to help minimise any potential harm and consequences later on in the development process. While problems still arose and caused delay with the project, they were minimised where possible, and resolving these problems while still adhering to the project deadlines helped me to improve my skills of working under pressure, as well as making me more familiar with issues associated with all the different technologies and tools that I used, which I believe is very useful knowledge to have going forward in the future. Most testing was carried out in the development environment, Eclipse IDE. However, manual testing was also performed where appropriate.

Learning Outcomes

Technical Learning Outcomes

While completing my project, I gained exposure to new tools and technologies. While this proved challenging at times, it helped me to improve my ability to go and learn new things on my own using the resources at my disposal.

MySQL Workbench

MySQL Workbench was used to host the database of the application. I had no prior experience with this tool and found it quite challenging initially. The installation and setup of this tool was more complex than any database tools that I have previously used before, and I had to go and read tutorials and learn about MySQL Workbench before I could begin configuring my database in it.

Hybrid Encryption

I had no knowledge of hybrid encryption until I was in the middle of the development process, when I decided to use this technique in my application. I had to go and learn about how it worked and how to implement it before I could start coding it into my application. This took a substantial amount of time. This is something that I would change if I was starting over again. I would have done more thorough research initially with the intention of preventing changes and therefore, saving more time for further development of the application.

Sockets

A socket provides an endpoint for communication between two machines. I used sockets to perform client/server communication for the transfer of files between users. While setting up sockets is not an overly complex task, combining my encryption and decryption functions with the sockets proved quite a challenge, and took a substantial amount of time to get working. This was one of the biggest challenges that I faced throughout my project.

Personal Learning Outcomes

Working individually

Working individually on this project and being solely responsible for all the work and organisation involved proved a great challenge for me at times, but was definitely a positive experience overall. This project pushed me out of my comfort zone, forced me to improve my ability to work well under pressure, as well as improving my decision making skills for the future.

Learning more about my interests

Doing this project provided me with an insight into the entire application development lifecycle. This was a new experience for me, and it helped me to further realise which area I am most interested in. For example, I enjoyed designing the user interface, and would like to develop my skills further in this area in the future.

Conclusion

I have achieved my goals regarding functionality and learning outcomes for this project. I enjoyed the challenges brought before me and the opportunity to be centrally involved in an application for the entirety of the development lifecycle. I am now much more educated about not only secure file transfer, but also new security tools and technologies which I can use in my future career.

Acknowledgments

I would like to thank my supervisor Patrick Tobin for his support and guidance throughout this project.

I would also like to express my appreciation to Richard Butler and Joseph Kehoe for their help and feedback with issues during the project.

Declaration

- I declare that all material in this submission e.g. thesis/essay/project/assignment is entirely my/our own work except where duly acknowledged.
- I have cited the sources of all quotations, paraphrases, summaries of information, tables, diagrams or other material; including software and other electronic media in which intellectual property rights may reside.
- I have provided a complete bibliography of all works and sources used in the preparation of this submission.
- I understand that failure to comply with the Institute's regulations governing plagiarism constitutes a serious offence.

Student Name:	Aoife O'Brien
Student Number(s):	C00214279
Date:	20th April 2020
Signature(s):	Aoife O' Brien

References

Gloabalscape.com, 2020. *What is secure file transfer?* [Online]
Available at: < https://www.globalscape.com/solutions/secure-file-transfer> [Accessed 20th April 2020].