SECURE FILE TRANSFER APPLICATION

Research Manual

Author: Aoife O'Brien

Student ID: C00214279

Project Supervisor: Patrick Tobin

Recipient: Institute of Technology Carlow

Date: Friday 1st November 2019

Table of Contents

Abstract

The purpose of this research document is to determine the way in which I will create a secure file transfer system, while raising awareness about this important mechanism and why it should be treated as essential for businesses today.

Secure file transfer refers to the sharing of data via a secure and reliable channel, a concept that unfortunately is not always given the respect it deserves.

Do you send classified or confidential information in work? Have you ever stopped to think about how the data travels from you to the recipient, and is it safe?

If the answer is no, you're not alone. What led me to do this for my project is the fact that while the action of sending sensitive data is performed millions of times worldwide every day, many people do it without giving it a second thought. The fast pace of the working life today makes time very valuable. People often try to save time in any way they can. Unfortunately, one key area this time saving seems to harm is secure file transferring.

This paper gives a further introduction to this concept, offers some fascinating statistics, and gives the opportunity to learn about the different types of available solutions, the technologies involved, and the technologies that will be used in this project.

While this project will come with its challenges, I believe that it will allow me to learn new things and develop my practical technical skills and knowledge further while helping to promote awareness about a topic that I am very passionate about.

Introduction

The ability to move data reliably and securely from one location to another is an important key to success and survival for many companies. In businesses for which their primary product or service is data, this capability is even more critical.

For my final year project, I will be designing a secure file transfer system. I decided to do this because protecting sensitive data is of paramount importance today, and I don't believe that best practice is being used in a frightening number of organisations. This may be due to a variety of reasons, such as lack of awareness and education, lack of resources and much more. However, the handling of sensitive files and information should be a top priority for businesses, and the potential damage from the exposure of such files can often be far worse than the time, effort and money involved in putting a secure system in place.

In an annual report by Ipswitch File Transfer published by Info Security Europe (See Appendix A for the full report), they detail the results of a survey of over two hundred IT leaders and practitioners with security responsibilities regarding person-to-person file-sharing practices (Ipswitch n.d.). The results proved quite shocking.

In short, some of the main findings from the survey include the following;

- **Insecure methods are being used to send confidential files:**
  For example, 84% of the people surveyed send classified or confidential files as email attachments, 52% of which do so daily. These files can include things such as payroll information, customer data and business plans etc.
  Outdated methods such as File Transfer Protocol (FTP) are also still in use in some organisations, which causes a security risk.

- **Use of personal email:**
  Nearly half admitted to using their personal email to send company documents and data, more than two thirds of employees surveyed use USB drives, smartphones and other external devices to move or back-up work related files, and 31% of whom have lost an external device containing sensitive business information. One main reason outlined for this is that they find it faster and more convenient than using complex corporate tools.

- **Limited IT Management visibility:**
  IT Management have low insight into data movement in their company. Over 50% said that they have "no real visibility" into the file transfers happening inside and outside of their organisation.

<div align="right">(Ipswitch n.d.)</div>

In short, the aim of this project is to create a simple system which will protect users' data while it travels from point A to point B. I say simple because I understand that most people are unlikely to spend time using a product that they find confusing or difficult, as it's a waste of valuable time and people have many other things to do. Therefore, I want to focus on keeping my system simple and easy-to-use, while ensuring that it works properly and efficiently at its purpose of securely transferring files between users. By doing so, I hope to try and spread awareness and education by showing organisations how a secure system can be put in place to try and mitigate the above concerns as best as possible and the benefits of doing so. Through doing this, I will also be teaching myself, as I have never designed a system like this before and will be using some new technologies that I have not worked with previously.

This research paper is broken into several sections which discuss the different aspects around secure file transfers. The first section begins with some of the similar solutions available and identifies their potential strengths and weaknesses to aid in fine tuning my own system and making the best choices.

The next section provides an overview of the technologies involved in designing the front end of the system, how these technologies were decided upon and why.

After that, an overview of the technologies involved in the background of the system is provided along with the reasoning behind those choices.

The report finishes with my conclusions, a glossary, an appendix and a reference list.

Similar Products

Existing solutions currently available on the market include;

Go Anywhere Managed File Transfer Solution

Go Anywhere is a service designed by the company HelpSystems that provides a paid managed file transfer service to organisations. This solution "automates and secures file transfers using a centralised enterprise-level approach and provides a safe and audited method for automatically transferring files within and outside of an enterprise" (Go Anywhere 2019).

Strengths

Flexibility: This MFT solution has the capability to be deployed in different types of environments including on-premise or in a cloud solution, as well as running on a variety of platforms such as Windows, Linux and more (Go Anywhere 2019).

Weaknesses

Cost: In my experience of working with such solutions previously, I understand that they can sometimes be expensive to purchase and maintain, which can often be difficult for small and medium sized enterprises.

Size: Go Anywhere also provides a variety of other solutions, which could mean that certain resources may not always be as freely available as they may be with a provider selling only this one service, for example online support.

LiquidFiles

"Liquid Files is a *Virtual Appliance that you install in your VMware, Microsoft *Hyper-Visor, *Xen environment, in your own private Amazon EC2 Cloud, or if you prefer on a dedicated server. LiquidFiles aims to fulfil all needs most organizations need to Send, Receive and Share Files of any file size in and out of your environment" (Liquid Files 2019).

Strengths

Ease of Use: Due to using this virtual appliance technology, this solution appears to be particularly easy to set up and run.

One Product Company: Liquid Files is a single-product company, meaning that they focus solely on this one solution and making it the best that it can be.

Flexibility: This solution can be installed on a choice of supported platforms as listed in the above website statement.

Weaknesses

Size: Given the fact that this organisation is internationally based and has worldwide customers, it could prove difficult to provide more personalised service to clients and to provide fast online support to all customers.

Front End Technologies

The following table lists the main modules of the system, followed by a brief description of each module:

Modules
Registration
Login
Send a file
Receive a file
Notification message
Sign Out

Registration: Users will register once with the system.

Login: Users will login to the system using their username and password.

Send a file: Users will be able to select the file that they wish to send, choose an encryption algorithm and enter/select the person that they wish to send the file to.

Receive a file: Users will receive a file from a sender and will decrypt it using the equivalent decryption algorithm to the encryption algorithm used by the sender.

Notification Message: A sender will receive a notification message to let them know that their file has been successfully received.

Sign Out: Users will securely sign out of the system once finished transferring files.

Programming Language

I will be using Java to design my frontend in the form of a *graphical user interface (GUI). The user interface will facilitate the above operations.

I chose this language because it is;

Cross-Platform: Java offers cross-functionality between a variety of *hardware and *software platforms as well as any Java compatible browser. This allows for easy movement from one computer system to another, which is a key characteristic that I am hoping to implement into my product, instead of narrowing it to one platform.

Distributed: Java was designed with networking in mind, meaning that it makes it relatively easy for computers to communicate and cooperate.

Secure: Important Java elements were developed with security in mind, including its compiler and interpreter. I think that this language is a good fit because my project is focused around security, and I can build on this throughout the development stage.

Robust: Java is a very reliable language. This may be accredited to the fact that it was designed to be simple and easy to use, and also given its maturity, any issues associated with it have been widely identified and remediated, meaning it is a very stable choice.

Well Known: Given the popularity of Java and the length of time it has been used in industry, it has a very large community of users and therefore a large support network.

However, Java is not perfect, just like with any programming language. For example, its performance can be significantly slower sometimes and potentially more memory-consuming than other languages. Depending on which Java version is used, the look and feel of a graphical user interface (GUI) can also differ from other applications.

That said, from my research, I have found that it is currently the best choice for me.

Java Toolkits

Within Java, there is a series of different collections of components and widgets, called toolkits, which can be used specifically to design a graphical user interface (GUI). I compared different Java toolkits to determine which option is best for this project. I narrowed it down to two, and then compared them further in more detail.

The two most suitable toolkits are;
- Swing
- JavaFX

Swing and JavaFX are graphical user interface (GUI) toolkits. Swing is one of the oldest toolkits while JavaFX is one of the newest. Some people debate that JavaFX is a replacement for Swing, while others acknowledge it as a new toolkit added to the collection that offers more modern functionality. Either way, Swing is still in use and according to its creators Oracle, "will remain part of the Java Standard Edition (SE) specification for the foreseeable future" (Oracle 2019).

I will be designing my user interface (UI) using Swing for the following reasons:

- As Swing is older and more developed than JavaFX, it contains less bugs and other issues.

- Swing has proved faster than JavaFX in certain circumstances, specifically on the Linux platform (Zara, S. 2018).

- I have previous experience using Swing, which will allow me to spend more time developing and improving the system instead of trying to learn a new language at the same time.

Given the time available for the project, I want to place greater focus and resources on the backend instead of the user interface, as what happens behind the scenes is of greater importance and is my main priority. If time allows, I will then work on further perfecting the appearance of the user interface.

It is possible to use both Swing and JavaFX in collaboration, so I can implement components of JavaFX if necessary for certain objectives, as they can work together.

Platforms

Another area that I investigated was which platform would be the best choice to create the project on. I looked at the two largest platforms used in industry today, which are Windows and Linux.

As I use Windows on my personal PC, I decided to install a Linux *virtual machine in a virtual environment in order to try Linux out before making a decision. After researching and speaking to my supervisor about Linux, I installed a Linux Mint virtual machine on my laptop. Linux Mint is a modern, easy-to-use and customisable Linux distribution.

In an attempt to identify which platform is most prominent in industry, I tried to compare statistics based on the market share of each platform.
However, given the large variety of devices available, these figures can prove difficult to measure.
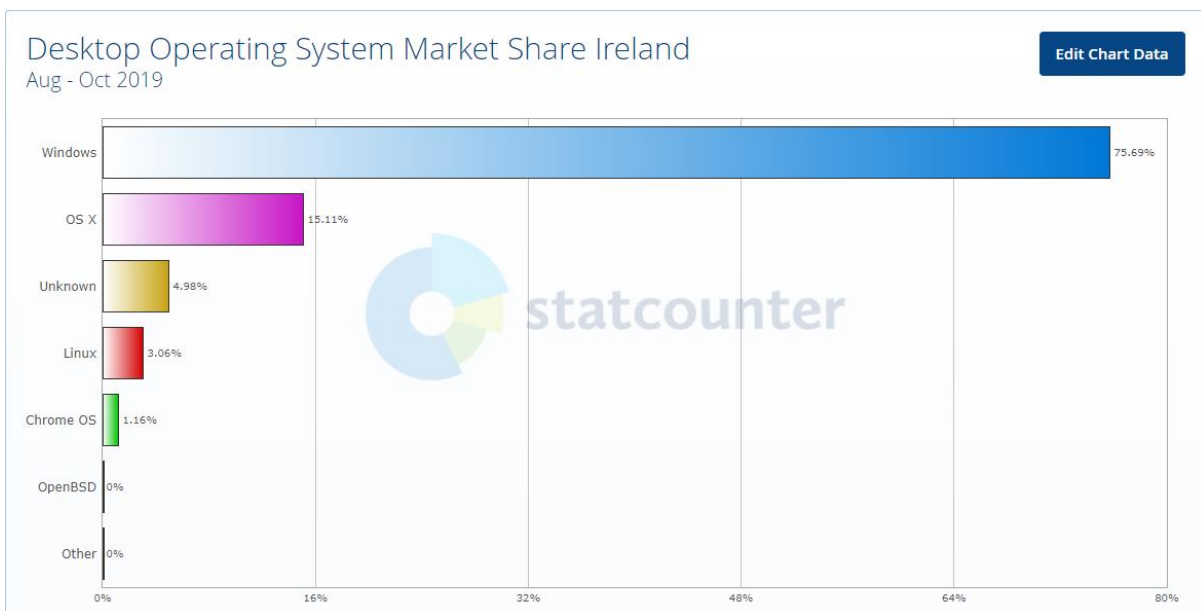
From the sources currently available, the following chart shows the operating systems market share for desktops in Ireland throughout the previous six months, from April 2019 to September 2019:
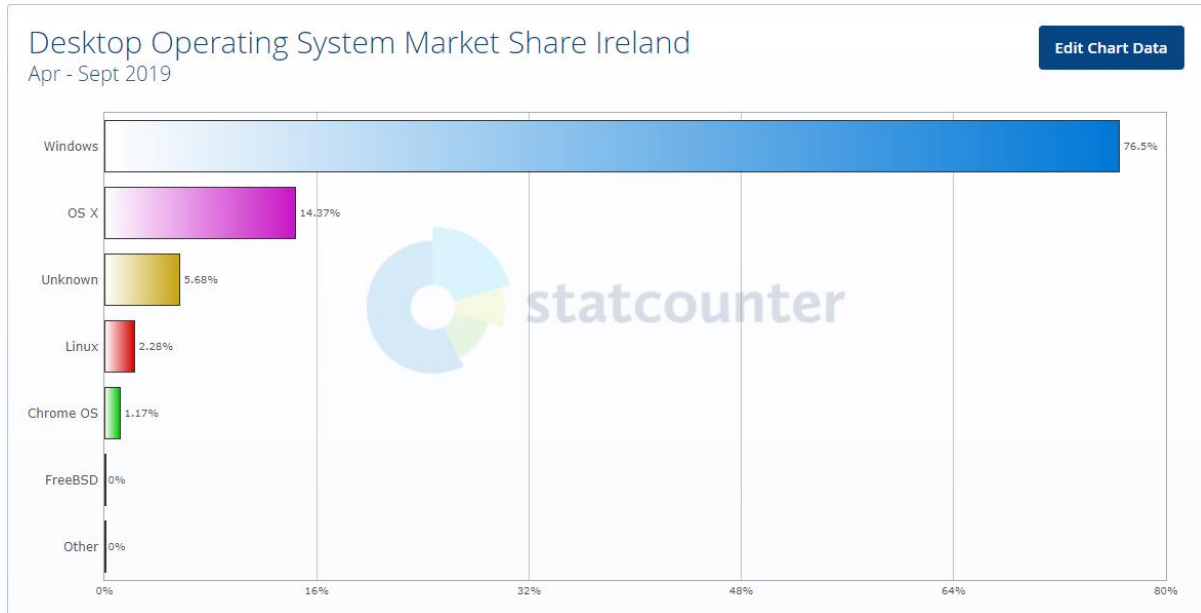
(StatCounter 2019)

The next chart shows a substantial 0.78% increase in Linux usage from August 2019 to date:

(StatCounter 2019)

From my research, it is obvious that Windows currently dominates the market when it comes to desktops and laptops.

However, it is also obvious that Linux is not going anywhere, and will only become more popular in the future. While not as commonly used as Windows on computers, Linux should be considered for its popularity in both the Android mobile market and the server's market. Linux definitely has its strengths and advantages in certain areas of operation.

Based on the current statistics that I have, I decided to create my system using Windows. If time allows towards the end, I will edit it as necessary to make it work on Linux also.

Notification Message

A message will be implemented for the sender of the file to receive upon successful transfer of their file. I intend to use Java to perform this action.

Back End Technologies

The following image lists the main components that will be used to perform the operations of my file transfer system:

Components
Database
Server(s)
Encryption
VPN Tunnel
Decryption

Next, I will provide a run through of the above technologies:

Database

As my system will contain both a registration and a login module, sensitive user information will be involved. To store the user credentials securely, I will use MySQL. MySQL is an *open-source database management system developed by Oracle. It is one of the world's most popular databases and is reliable and has a strong track record for its performance.

In order to configure my Java application to connect to the database, I will use the Java Database Connectivity (JDBC) application programming interface (API). This is the industry standard for database connectivity of this type (Oracle 2019).

Encryption & VPN Tunnel

In order to transport the files as securely as possible, I intend to use *encryption and a *Virtual Private Network (VPN) tunnel to do so. A choice of approximately two encryption algorithms will be given to the sender before sending their file. The two algorithms will be *The Advanced Encryption Standard (AES) and *Twofish. A third option will be added if time allows.

I will be using AES because it is one of the most secure algorithms available and is used in industry worldwide.

I chose Twofish because it's lightweight and not very resource intensive. This cipher works well on machines with a smaller or less powerful CPU. Furthermore, "this form of encryption is license free and unpatented so it can be used without restriction" (TopTenReviews 2017).

To implement stronger security, I may also use the Java Socket Secure Extension (JSSE). This extension offers a wide range of capabilities based around security, such as features for encryption, client and server authentication as well as file and message integrity.

Decryption

*Decryption will take place at the file receiver's end each time a file is transported. The algorithm used will be the decryption equivalent to the encryption algorithm that the sender used.

Server

A server will be necessary to perform the relevant operations between the sender and the recipient. I intend to use one server to perform the different necessary roles, such as VPN functionality, file server and application server roles. The reason for this is to save valuable time and resources.

Depending on the size of the organisation, this choice may not be an option, as it can cause limitations surrounding performance and other issues. This option is very much based towards small to medium sized enterprises at this moment in time. The aim is to create an enjoyable and easy to use system in a very affordable manner.

Conclusions

The secure file transfer system will be designed using the technologies outlined above. Java and its relevant libraries, extensions and toolkits will be used to design the user interface.

The components and processes involved in the backend of the system will receive the highest priority, as the security features of the system are the focus of the project.

Certain features including the system's implementation in the Linux platform, and the potential third encryption algorithm option for the senders will be implemented if time allows once the main features are finished.

The ultimate goal of the project is to securely transfer data from a sender to a receiver, while protecting the *confidentiality and *integrity of the data.

Some of the market solutions available are discussed at the beginning of the report. The system being designed aims to achieve similar goals as the outlined solutions. However, given the difference in time and resources available, this system will be based on a smaller scale. The scope is primarily based around small to medium sized enterprises, and potentially even individuals also. As mentioned in the previous section, an enjoyable, easy to use, secure and affordable system is what I wish to achieve.

A secure file transfer solution is essential for businesses today in order to prevent attackers from intercepting, stealing or altering your private information as best as possible. In my opinion, data is now one of, if not the biggest asset that companies have, and that data must be managed responsibly and appropriately. Something as simple as sending an unencrypted file over an unsecure method by mistake or without thinking has the potential to cause significant harm to your business.

Glossary

The Advanced Encryption Standard (AES): A secure encryption algorithm.

Application Programming Interface (API): An interface that allows for communication between a client/user and a server. Its purpose is to allow for easier creation of applications which access other services.

Confidentiality: The practice of keeping private information private and ensuring that it cannot be seen by anyone who should not see it.

Database: A collection of organised data stored in electronic form and accessed by a computer.

Decryption: The reverse process of encryption. This involves changing the encrypted data back into a human readable and understandable form using a special key.

Encryption: A cryptographic process of hiding the contents of a message/file in such a way that only authorised parties can access the information.

File Transfer Protocol (FTP): A protocol used to transfer files between a user's device and a server on a computer network.

Graphical User Interface (GUI): An interface designed to allow users to interact easily with a computer by making choices from menus, icons or windows (Merriam Webster 2019).

Hardware: Refers to the physical elements that make up a computer.

Hypervisor: A hypervisor is a hardware virtualisation technique that allows multiple guest operating systems (OS) to run on a single host system at the same time. The guest OS shares the hardware of the host computer, such that each OS appears to have its own processor, memory and other hardware resources (Techopedia 2019).

Integrity: The practice of ensuring that data has not been manipulated or changed in any way throughout its life cycle.

Open-source: Refers to products or software whose source code is available to the public free of charge to use, modify or distribute.

Software: A generic term used to describe computer programs, which are a set of instructions to be performed by a computer.

Symmetric block cipher: An algorithm used to encrypt blocks of data using a transformation which is specified by a secret key shared between the parties involved.

Symmetric Encryption: Occurs where the same secret key is used to both encrypt and decrypt the data being shared.

Twofish: A *symmetric block cipher.

Virtual Appliance: Pre-configured software including operating system (Liquid Files 2019).

A software application residing and operating in a preconfigured virtual environment or platform. Virtual appliances are accessed remotely by users and do not require locally-installed hardware (Techopedia 2019*).*

Virtual Machine: A virtual machine (VM) is a software program or operating system that not only exhibits the behaviour of a separate computer but is also capable of performing tasks such as running applications and programs like a separate computer (Techopedia 2019).

VPN Tunnel: A secure channel between two devices or networks used to send sensitive data. These channels are most often encrypted.

XEN Project/Environment: A hypervisor that allows multiple computer operating systems to execute on the same computer hardware concurrently (XEN Project 2003*).*

Appendix

Appendix A: Ipswitch File Transfer Survey Report
Available at: [Online]
<https://www.infosecurityeurope.com/__novadocuments/58365?v=635430219816700000>.

References

GoAnywhere.com, 2019. *GoAnywhere Managed File Transfer (MFT)* [Online]
Available at: <https://www.goanywhere.com/solutions/managed-file-transfer> [Accessed 24th
October 2019].

Info Security Europe, n.d. *Are Employees Putting Your Company's Data at Risk?* [Online]
Available at: <
https://www.infosecurityeurope.com/__novadocuments/58365?v=635430219816700000>
[Accessed 29th October 2019].

Linux Foundation, 2003. *WHAT IS THE XEN PROJECT?* [Online] Available at: <
https://xenproject.org/about-us/> [Accessed 26th October 2019].

LiquidFiles, 2019. *LiquidFiles* [Online]. Available at: <https://www.liquidfiles.com/>
[Accessed 24th October 2019].

Merriam-Webster.com, 2019. *Graphical user interface* [Online] Available at:
<https://www.merriam-webster.com/dictionary/graphical%20user%20interface> [Accessed
27th October 2019].

Oracle.com, 2019. *Java SE Technologies – Database* [Online] Available at:
<https://www.oracle.com/technetwork/java/javase/jdbc/index.html> [Accessed: 01st
November 2019].

StatCounter, 2019. *Desktop Operating System Market Share Ireland Apr – Sept 2019*
[Online] Available at: <https://gs.statcounter.com/os-market-share/desktop/ireland/#monthly-
201904-201909-bar> [Accessed 28th October 2019].

StatCounter, 2019. *Desktop Operating System Market Share Ireland Aug – Oct 2019* [Online]
Available at: <https://gs.statcounter.com/os-market-share/desktop/ireland/#monthly-201908-
201910-bar> [Accessed 28th October 2019].

Techopedia.com, 2019. *Definition – What does Hardware (H/W) mean?* [Online]
Available at: <https://www.techopedia.com/definition/2210/hardware-hw> [Accessed 27th
October 2019].

Techopedia.com, 2019. *Definition – What does Hypervisor mean?* [Online]
Available at: <https://www.techopedia.com/definition/4790/hypervisor> [Accessed 27th
October 2019].

Techopedia.com, 2019. *Definition – What does Software mean?* [Online]
Available at: <https://www.techopedia.com/definition/4356/software> [Accessed 27th
October 2019].

Techopedia.com, 2019. *Definition – What does Virtual Appliance mean?* [Online]
Available at: <https://www.techopedia.com/definition/13705/virtual-appliance> [Accessed
27th October 2019].

Techopedia.com, 2019. *Definition – What does Virtual Machine (VM) mean?* [Online] Available at: <https://www.techopedia.com/definition/4805/virtual-machine-vm> [Accessed 27th October 2019].

Tech Terms.com, 2019. *Firmware* [Online] Available at: <https://techterms.com/definition/firmware> [Accessed 24th October 2019].

TopTenReviews.com, 2017. *Which Types of Encryption are Most Secure?* [Online] Available at: <https://www.toptenreviews.com/secure-encryption-methods> [Accessed 29th October 2019].

Zara, Steve, 2018. *..Swing has significant advantages:* [Online] Available at: < https://www.quora.com/Which-are-the-mainly-differences-between-Swing-and-JavaFX-Do-I-have-to-learn-Swing-first-or-can-I-go-for-JavaFX-directly> [Accessed 27th October 2019].