Year 4 Project Proposal

SECTION A:

Project Title: Password Manager with Cloud-Free Synchronization
Student Name: Dean Lynch
Student ID: 15359921
Stream: CASE4
Project Supervisor Name: Brian Stone

SECTION B:

General area:

I plan to develop a password manager with a locally stored database that can be easily synced across devices without the use of 3rd party cloud services.

A password manager is a program used to store, manage and generate passwords. There are two common implementations of password managers:

1. An online service offered through a web portal:
    a. Users connect through a web page or browser extension
    b. The database is stored online, i.e. not locally on the users device.
    c. User only has to remember a username/password, they can access their database from most devices.
    d. Examples: LastPass, Keeper
2. A locally installed application, with a locally stored database.
    a. Users run an application locally on their device.
    b. The application reads a locally stored database.
    c. User has to handle synchronization of their db themselves, or host it on a server provided by the password manager.
    d. Examples: Keepass2, Enpass

The problem with password managers that implement online/cloud database storage is that the user has no control over how or where the password database is stored.
The problem with a locally installed application that the user is left responsible for keeping the database synced across multiple devices.

Outline:

Background:

I've been using a password for over two years, and I have used both an online service (LastPass) and a locally run application (KeePass). I currently use KeePassXC. Previously I synced my password database across devices using DropBox. Over the summer I discovered Syncthing, a peer-to-peer file synchronization application. I now use Syncthing to sync my password database across devices. The use of KeePass alongside Syncthing gave me the idea to combine the password management and synchronization service into a single application.

Achievements:

There are two high level requirements I have for the application:

- Full control of where and how the database is stored by implementing a locally stored database, i.e. the database is only kept on devices that it will be accessed on.
- The ability to sync the database between devices without the use of 3rd party cloud storage.

The target users of the application will be people who are concerned about their privacy and security; people who want to have full control of their data.

Justification:

I am yet to find a password manager that provides a locally stored database with synchronization across devices without the use of cloud storage; this is the niche in the market I intend to target with this project.

Programming languages:

- Java
- TypeScript/JavaScript

Programming Tools/Tech Stack:

- Web Sockets
- Electoron/JavaFX/Swing (Undecided)
- VirtualBox
- Spock
- IntelliJ

Learning Challenges:

CA40010 Cryptography & Security Protocols was cancelled this year, which is unfortunate because it could have really helped with my project. This means that I will have to research some of the topics covered in the module myself. A very high level of security is required for this application, therefore I will have to constantly familiarise myself with any flaws or weak points that are included with any of the technologies I have used.

While I have worked with very large Java projects in the past over my INTRA placement, I have never created one from scratch myself.

I've had experience building a frontend for a web application, but never a Java application. Since this is completely new to me I will have to weigh up the pros and cons of each of the different implementations of a Java frontend, as well as pay special attention to any security drawbacks some of them may contain.

Hardware/Software Platforms:

- My personal laptop for development and testing.
- My personal desktop for running virtual machines.

Special Hardware/Software requirements:

None.