Jacob Hoog, 18072523

ECE 4220 Final Project Proposal

Username-Password Security System

**Addressed Topic**

Account security is an incredibly important area of any technology based enterprise. Banks and other large businesses are entrusted with protecting the investments made by customers by having proper account protection. As stories of companies having their information stolen continue to appear, I believe that data security has continued to grow in importance as technology progresses. My objective with this project is to create a security system which uses an account name and password pair to identify individual users. The system will have access to a list of accessible account and checks if the username input is recognized before prompting a user for a password. Each password will be a sequential order of button presses that, when input correctly, will allow a user to view their personal data. The current design of this project does not use the FairCom database system and a more in depth look at the implementation of this system is provided in the methodology section of this proposal. This security system will be connected to a simulated bank system to show its capabilities during testing.

**Related Systems**

The username and password pair system is the main approach to data protection used by many websites and companies. These systems also may include a password recovery system using a preset question that was made during account creation. Other more recent security systems include fingerprint and face recognition on phones. Sometimes account information is stored physically and is read in using a scanner, such as with credit cards and identification cards. All the above mentioned systems are also effective, but a username password system is more easily upgraded to higher levels of security by increasing the length of passwords are placing requirements on what inputs are allowed within a password.

**Goals**

The initial short term goal for this system will be implementing the list of accounts. This will need to work correctly to allow any of the other features of this security system to function. Another short term goal for this project is to be able to manage the passing and searching of user information in a timely manner. Missing deadlines such as password input would be a serious issue in this system, so creating a real time program would work best in this system. A more long term goal for this design is to make it accessible from multiple systems located miles apart from each other. This may be challenging for the demonstration program described in this proposal, but future implementations could include a feature similar to this. The final goal for this project is a functioning user security system that contains all the necessary functionality to protect a user’s data.

**Benefits and Expectations**

A benefit that comes with username password pair systems is that it is easily adaptable to required situations. Should this proposed system need to be modified to fit some data other than the demonstrated banking example, very little editing would be needed to adjust to the new system outside of changing how the data is brought into the system. Another benefit of this design is that it is not hardware intensive to implement. The majority of the work in this project is done through the software programs and the coding, which could make it more desirable compared to other security systems like card scanners. The expected outcome for this project is a functioning username password pair security system, which will be adaptable to future designs once fully completed.

**Constraints and Specifications**

The largest constraints for this security system will be hardware related. While researching potential components for this project, I was unable to find a readily available keypad that could be connected to the ts7250 circuit board provided. For this current design, an auxiliary board will work as the number pad, but future versions of this design could be upgraded to a more complex keypad. The number of stored accounts could also affect response speed if the number grew to a large enough amount. For this demonstration model size should not be an issue, but for future implementation a sorting method on account names could greatly increases access speed.

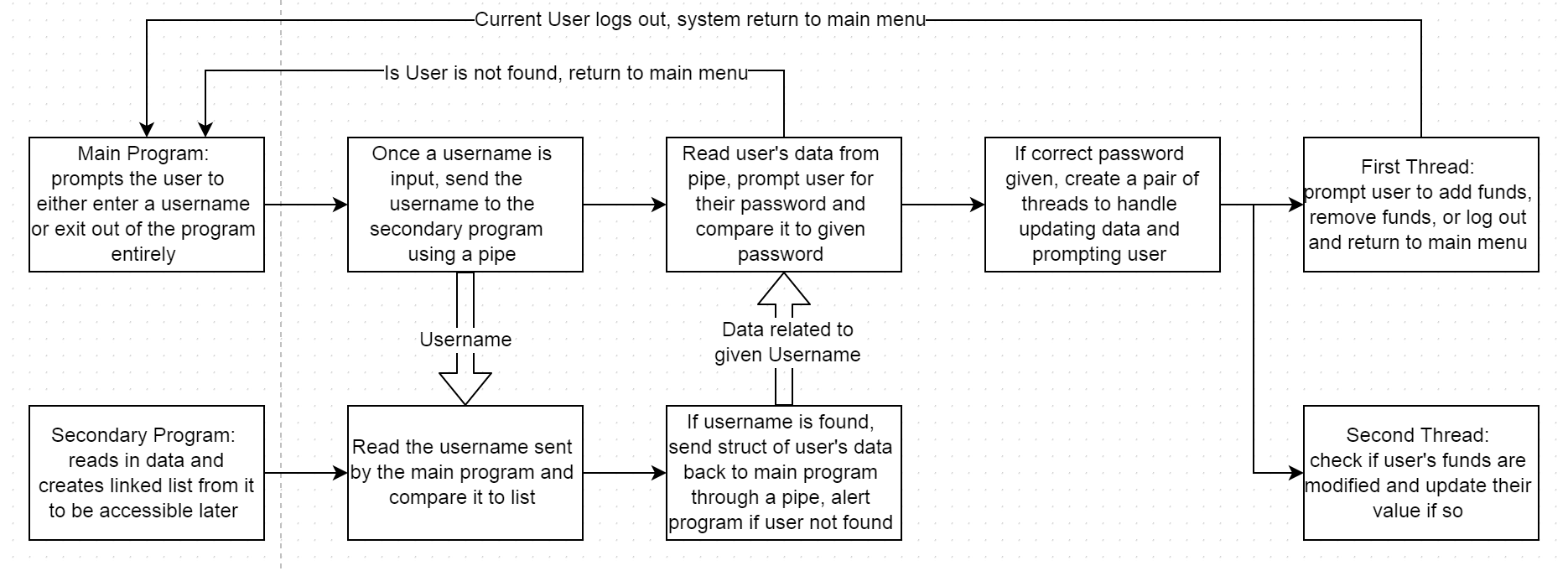
**Assumptions**

To use this version of the security system, it is assumed that computer setups using it will have access to the ts7250 circuit board and the auxiliary board containing push buttons and the connecting ribbon wire. For this demonstration version, it is also assumed that users have the necessary access requirements to log into the nfs1 server and ts7250 circuit board, as the program will be designed to run through these.

**Methodology**

This system will be a combination of two programs which will pass data to one another. The main program will present login features to the user including prompting for the username on the desired account and exiting the system. The secondary program creates a linked list of accounts which can have their data piped to the main program when required. Once a username is input, that username will be sent off to the secondary program which will attempt to locate the related account. If found, the data related to that specific account is sent back to the main program and the user is prompted to input their 4 digit password via sequential button presses. If the username is not recognized by the system, the program will send the user back to the main menu. When the user inputs the correct password for their given username, they are then given access to modify the funds of their account and can exit back out to the main menu whenever they wish. The updating of account values such as funds and handling of user inputs can be split into two threads and regulated with a semaphore to ensure the system does not attempt multiple actions on a variable at one time. Various aspects of embedded systems that we have learned from class are presented in this design. The passing of data between the two projects represents the ideal of task communication and the splitting of tasks into two separate threads within the main program utilizes the multi-threading concepts learned in class. The real time ability of embedded systems is also touched upon in the semaphore used in managing the two simultaneously running threads. A flowchart of this project noting all the key points within the program is available in the timeline section of the proposal.

**Timeline and Milestones**

In the below chart, the black arrows represent the progression of the system through its various key phases and the white arrows represent the pipes sending data between the two systems.

**Strengths and Limitations**

The main strength of this system is in its versatility. Unlike keycards and fingerprint scanners, a password based security system can easily be strengthened by simply increasing the length of the passwords or by expanding the characters usable within a password. More advanced password based systems can include encryption capabilities to even further protect user data. The relatively low hardware requirement of this security system is also a strength. When compared to the scanners needed for ID cards and fingerprint based security systems, the circuit boards needed for the system outlined in this proposal are more easily addable to a larger system. A limitation on the username password pair system is access time. If the catalog of registered usernames becomes too large, response time when searching for a specific user can suffer. The number of buttons available on the auxiliary board is also a limitation of this current design. To increase the number of characters available to a password as described previously, a more complex keypad would be required.