**ECE 412**

**Product Design Specifications PDS**

**Identity Authentication**

**Introduction**

Our project is to create an identity authentication device. It will be used to authenticate (or allow access) users logging into a laptop. It will have three different inputs. One of the inputs will be in the form of biometric information. This will be achieved by performing a fast fourier transform on the user(s) speech and determining whether it is consistent with that of an authorized user. The range of frequencies that we will focus on is between 50 Hz and 1kHz. These frequencies are consistent with that of male and female speech. Once the user is identified, they will have to enter their pin. Each authorized user will have their own unique pin which they must enter once prompted to do so by the program. If the user meets both of these criteria, the program will access the current GPS location and display this information.

**Needs Statement**

?

**Objective Statement**

We want to create secure access in a very connected world.

**Market Analysis**

The number of people that have had their data breached has increased exponentially throughout the years. Big companies such as eBay, Equifax, Marriott International, and Heartland Payment Systems have all been compromised to some extent. More notably, the department of defense was hacked back in the late 90’s. In a world revolving around technology, it is frightening how our information can be compromised with the snap of a finger. Our project aims to put the consumer at ease. This product cannot prevent your data from being compromised but it will add another layer of protection. With this added measure of security, we hope to prevent you from being the next victim of a cyber attack.

This (project) is for people who are connected to the rest of the world through their laptop, so everyone. We plan on starting small with our client and hopefully reach anyone who wants a better sense of security. Our competition consists of

**Requirements**

Our device (or program/code in this case)...

**MUST**

* Accept a pin
* Analyze speech by means of a fft
* Identify new or returning users
* Print or receive GPS Coordinates
* Voice and Pin combine such match from the user

**SHOULD**

* Can be offline from initial voice
* Voice data frequency stored in the device
* Allow a new user (enter a new voice and a new pin)

**MAY**

* Indicate who the user is
* Indicate the user can have access

**Block Diagram**

**Design Specifications**

* Raspberry Pi (Possible Processor)
* Build Microphone (Possible mic for voice recognition)
* 3x4 4x4 Raspberry Pi Keypad (Possible keypad pin number)
* GPS Module (tracks down the current location, specifically the coordinates)
* FFT (Fast Forward Ttransform)

Success:

How many tries of detection of prevention authuietion?

* Keep in mind separate test cases

Correct authiention, identify an authorized person [True Positive]

Correct prevention, identify an unauthorized person [True Negative]