Team 11: Multi-Factor Identity Authentication

Authors:
Tamarr Stigler-Flores
Danny Wu
Uzias Cruz Asuncion
Navid Karamichamgordani

January 10, 2021

Version 1.0

Table of Contents

Executive Summary

We will create a mockup two-factor authentication program. The two authentication factors are pincode and voice recognition; Fast Fourier transform analysis handles voice recognition. Moreover, the program permits access if and only if user authentication was successful. Upon successful authentication, the user's GPS coordinates will be obtained and displayed by the program.

Product Design Specifications PDS: Identity Authentication

Concept of Operations

For our project, our team will develop a mock-up multi-factor authentication program. The program has three inputs and one output. The inputs are a 4-digit pin, user voice, and GPS signal. The output is a welcome message that includes the user's GPS coordinates. In addition to the inputs and output, the program contains a database containing authorized users' information, such as pin # and user voice FFT analysis results.

The program prompts the user to enter the 4-digit pin, and it is compared to existing profiles in its database. The user gets three attempts, and if failed, the program locks the user out for 10 minutes and starts over. If the pin# matched, the program prompts the user to say a phrase in English, and it performs Fast Fourier Transform (FFT) analysis obtaining the highest three peak frequencies. The result is compared to existing profiles in its database. If the FFT comparison failed, the program asks the user to repeat the phrase; the user has three attempts only, and after that, it locks the user out for 10 minutes and then starts over by asking the user pin #. Suppose FFT analysis matches. In that case, the program obtains the user's GPS coordinates from a GPS module and outputs the GPS coordinates on the console (laptop, in this case).

Stakeholders

- John Acken (Sponsor)
- Malgorzata Chrzanowska-Jeske
- Project Team
    - Danny Wu
    - Tamarr Stigler-Flores
    - Navid Karamichamgordani
    - Uzias Cruz Asuncion
- People who connects to the internet or a computer (Users of the system)

Needs Statement

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.

Objective Statement

The objective of this project is to create a functional program to be part of a security system that checks multiple factors. These factors are: a password (information), the user's voice (biometric), and location.

Market Analysis

This software program is for people who are connected to the rest of the world through their laptop or desktop. We plan on starting small, by meeting our client's needs, and hopefully reaching everyone who wants a better sense of security. Our competition consists of other companies who have created some form of authentication. There are various technologies in the market.

There are many companies that have their own source of multi-factor authentication. Apple decided to do an authentication by getting a verification code and signing in with a two-factor authentication. It's a six digit verification approved from email or text. Google decided to do an authentication by using a generated password and a characterized code to gain access to approval. Trusona is a passwordless code authentication that approves access into multiple security sources such as online shopping and atms. ExpectID is a fast authentication program that verifies customer's address and name with various online databases. These are our competitors. We hope to make our program much more affordable than our competitors. Since our design is mostly software, it is projected to be at a much lower price than competitors. This would be very affordable for the average person.

Requirements

Our design ...

MUST

- Accept a pin [Four-digit Pin]
- Analyze speech by means of a FFT
- Identify new or returning users
- Create an initial database for every user's frequency and pincode
- Receive and output GPS coordinates
- Check if voice and pin match the corresponding user
- Indicate who the user is

SHOULD

- Can be offline from initial voice
- Support cross-platform
- Voice frequency data stored in the device

MAY

- Allow new user to register
- Store new user pin and voice
- Add the new user to list of the current users

Design Specifications

- Hardware
    - Available PC or Laptop
    - A Build-in Microphone (Possible mic for voice recognition), or portable microphone
    - Keypad/Keyboard
    - GPS Module (tracks down the current location, specifically the coordinates)
- Software
    - Development Environment: Python
    - Frequency Range : 125-10kHz

Deliverables

- Project Proposal
- Weekly Reports
- Final Report
- ECE Capstone Poster
- User Manual
- Finalized Program

Initial Product Designs

For this capstone project, we plan on creating a complete software that will use multi-factor authentication to provide access to users on their devices. The factors that will be used for authentication are: biometric (something we are), some password (something we know), and location (where we should be). For our design, we will be utilizing a voice input for speaker recognition, a simple 4-digit pin, and GPS coordinates for the user's current location. When attempting to be authenticated, the inputs are being compared to existing profiles in an initial database. This will be constructed using Python which has many libraries available that can be utilized and simplify the project in order to fulfill the requirements.

The password will just be a simple 4-digit number. The user will first be asked to enter their pin which is compared to their profile in the initial database. They are allowed up to three attempts before being kicked and locked out for a period of time, around 10 minutes.

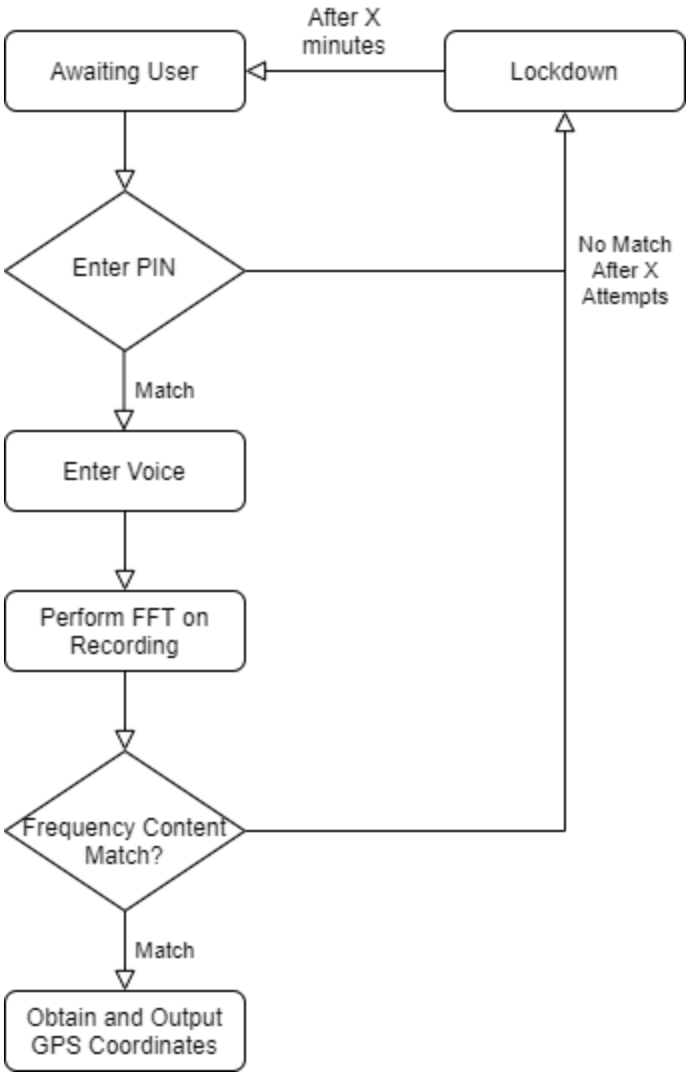
After the PIN authentication has been passed, the voice input for speaker recognition will be performed by first asking the user to say a particular phrase. Once a recording has been taken, a Fast Fourier Transform (FFT) will be performed to analyze their voice. From the analysis, we will be taking the frequencies in which there are high peaks and comparing these results to the stored peak values of the user's profile. If the user passes both verification steps, then their current location will be found using the GPS from their device and the coordinates will be displayed by the program.

Our first risk is the programming language. From initial research, it appears that Python may be the most effective programming language to use in order to fulfill the requirements. Though the team does not have great experience with the language, we will overcome this through individual practice and research in order to complete the project.

Another big risk of this project will be the voice verification process. We need to find a way for the user to input their voice, have that recording be analyzed and using that analysis in order to match them to the same person. As we are unfamiliar on the topic, we need to conduct a considerable amount of research to find a starting point to base the design off of. With that, this part of the project is likely going to be the most difficult part considering the things required in order to accomplish the tasks. We will need to conduct many experiments in order to achieve an acceptable true positive and true negative rate compared to the false positive and false negative rates. The question now is how will we conduct these tests and what amount should we take from the FFT analysis to be used for finding a profile match? To fix these issues, the current plan is to have the team use their own voice recordings to attempt to match themselves with their profile. By going through many trials, we should ideally be able to find out how many peaks should be taken from the FFT to create matches. In addition, we will include the user's name as part of the phrase to be spoken for the input. We believe this may help in identification as a person'a name can be spoken in many different ways than the person would themselves in addition to the different voices people naturally have. Though now this also begs another question, what should the tolerance of ranges should be for each peak frequency as the exact frequency in which there is a peak may differ from each time it is spoken. This is also most likely to be solved during our experiments with what should be taken from the analysis.

A large risk for this project is finding a way to obtain the GPS coordinates of the device being used to gain access. Our group has done some research on the fft analysis and pin inputs but we lack in the methods of obtaining GPS coordinates. How can we access the users coordinates from our code? Will this process look different if they are running a different operating system? How can we achieve this offline? There is a lot of research and experimenting to do with the voice recognition and GPS coordinates but we believe we can deliver a working project by the end of the capstone.

Upon logging into their device, a user would be prompted to enter their PIN. After the input is given, the program would verify if they are the correct user to move to the next step otherwise would ask for an input again up to three times. Now verified, the program will now ask for their voice input and is allowed three attempts before they are kicked out of the login for 10 minutes. If the user is verified for both of these factors, then they now have access and the program will obtain and output their current GPS location. Programming in Python with Anaconda.



Back up plans

- Transition into a different language that has better capabilities
- Use different software (IDE)
- Buy physical GPS module to integrate into the design

Verification Plans

- Test GPS module and ensure it functions properly
- Test every module individually and verify functionality
    - Pin module: confirm it can accept, store and match pins
    - Voice FFT module: confirm it can perform FFT and compare the result with user FFT pre-saved result(s)
    - GPS coordinates module : correctly obtain GPS coordinates and is relatively accurate
- Combine all the modules and test the program.
    - Test with different users and verify it functions the way described in concept of operations and follows the project requirements

Project Management Plan

Timeline

- Provided in a separate file. Please see the attached schedule.

Budget and Resources

- A Windows 10 computer with internet access
- Portable microphone
- Work will be done at home
- 5 GPS Modules (estimate: $120). Sponsor committed this purchase

Team and Development Process

For this year's capstone our team members are Tamarr Stigler-Flores, Danny Wu, Navid Karamichamgordani, Uzias Cruz. Our educational background contains two Electrical Engineers students (Danny and Uzias) and two Computer Engineering students (Navid and Tamarr). Each student has their own specific skills to bring to the table.

Skills:

Tamarr Stigler
- Moderate level of C/C++ programming
- Moderate level of Python programming
- Soldering, Breadboard
- Positive ability of organization and scheduling
- Beginning level of Raspberry pi and Arduino

Danny Wu
- Organization and project management
- LTspice
- Sight experience with C programming
- Sight experience with arduino

Uzias Cruz
- Slight experience with arduino and Raspberry pi
- Moderate experience with C Programming
- Fundamental knowledge of electrical circuits

Navid Karamichamgorda

- Experience with Eagle and ProjectLibre
- Experience with C Programming
- Beginning Experience with Python Programming
- Experience with Raspberry Pi
- Basic Soldering
- LTspice

Roles:

Tamarr Stigler-Flores

- Create a program that involves identifying 4-digit code from a specific users
- Translate the C programming language to Python programming language
- Learn about FFT

Navid Karamichamgordani

- Create a python program that accepts a 4 digit pin number
- Create a python program that accepts an audio file, performs simple FFT on it and graphs the result
- Help with creating a python program that outputs GPS coordinates
- Research voice authentication via FFT
- Help with project schedule

Danny Wu

- Note taking and documentation
- Research/Work on implementing GPS. Obtaining/Outputting coordinates
- Assist in voice authentication

Uzias Cruz

- Research on FFT analysis implementation in Python
- Support in voice analysis module, testing and debugging
- Work on project schedule
- Help with GPS module testing and implementation

- Who is going to be the point person to be communicating with your industry sponsor and faculty advisor?

As a group, we decided to cycle group leaders to communicate with our industry sponsor and the faculty advisor. During the time between January to June, the team leader will be broken into four time slots approximately to 5 weeks. After each 5 weeks, a new leader will be assigned.

- What collaborations tools are you going to use?

The collaboration tools we plan to use are Github, Google Drive, and Slack. The slack channel is a source for all team members to communicate with each other and to set up meetings. Google Drive is a source to

organize files, documents and materials. Github will be the source to publicly display our capstone project. This contains our codes, puseducode, notes, and documentations.

Portland State UNIVERSITY

Navid Karamichamgorda <knavid@pdx.edu>

Approval for ECE412 team 11 Project Proposal

1 message

John M. Acken <acken@pdx.edu> Thu, Feb 4, 2021 at 7:43 PM
To: Navid Karamichamgorda <knavid@pdx.edu>, Danny Wu <wdanny@pdx.edu>, Tamarr Stigler-Flores <ericts2@pdx.edu>, Uzias Cruz Asuncion <uzicruz@pdx.edu>, Malgorzata Chrzanowska-Jeske <jeske@ece.pdx.edu>

To Prof Faust and Greenberg,
I am the sponsor for ECE 412 team 11
"Multifactor Authentication Program"
And I have reviewed their Project Proposal and I approve.

John M. Acken, PhD
Research Professor
Rm 20-03 FAB
Electrical and Computer Engineering
Portland State University
1900 SW Fourth Ave
Portland, OR 97201