Multi-factor Identity authentication Device

Background

Identity authentication is used to determine whether or not an individual should be granted access. The usual approach for a computer is a user name and password. The usual approach for crashing a check is a picture id. These are two different factors for identity authentication. The first factor is information (or what your know) the second factor is a biometric (what your are). Independent multi factors are used to increase the security for access control.

Problem

How can one have a very secure access in the connected world (whether into the internet or into a a portable laptop computer)?

Proposed solution

A portable multi factor authentication device based upon three independent factors. The device will accept a password from a keypad. The device will also accept a voice input for speaker identification. The device then outputs the current GPS coordinates. For speaker recognition, the first step is to do a simple FFT for the authorized speaker and then store that on the device. The next step is to implement a device that accepts a password (or pin) and checks that the password and the speaker id match the authorized list. The device then access the current location from a GPS device and outputs the GPS coordinates.

Deliverables:

Initial voice analysis step: Can be offline and the voice frequency data stored on device.

Build device that: accepts a pin, a voice, and gets GPS coordinates. The device must check for matches,

Final report includes evaluation of the accuracy (measured by match and mismatch rates) for various threshold settings and demonstrated experiments.