1-Step, 3-Factor Authentication with Custom-Fit, In-Ear EEG

ffff

February 5, 2017

Abstract

In this paper, we present a system that provides 3-factors of authentication (knowledge, posession and inherence) in a single step, using brain-based authentication via a custom-fit, in-ear EEG. Across all subjects, we achieve a best-case XX% false acceptance, XX% false rejection rate with data from only one earpiece. In a preliminary test of an "imposter" spoof attack, we find a 0% false acceptance rate. Conclusions and relevance.

1 Introduction

It is well appreciated by experts and end-users alike that strong authentication is critical to cybersecurity and privacy, now and into the future. Unfortunately, news reports of celebrity account hackings serve as regular reminders that the currently dominant method of authentication in consumer applications, single-factor authentication using passwords or other user-chosen secrets, is faced by many challenges. Major industry players such as Google and Facebook have been strongly encouraging their users to adopt two-factor authentication (2FA). However, the need for users to submit two different authenticators in two separate steps has frustrated wide adoption, due its additional hassle cost to the users. For instance, the popular Apple iPhone has already implemented the necessary technologies to support device unlock using either a user-selected passcode or a fingerprint. Therefore the device could easily support a two-step two-factor authentication scheme if desired. However, it is easy to understand why users would balk at having to enter a passcode *and* provide a fingerprint each time they want to unlock their phone.

In previous work, "one-step two-factor authentication" has been proposed as a new approach to authentication that can provide the security benefits of two- factor authentication without incurring the hassle costs of two-step verification. By employing consumer-grade EEG (electroencephalogram) sensing technologies, it was demonstrated in a 2013 passthoughts study that a user can submit both a knowledge factor (i.e., secret thought) and an inherence factor (i.e., brainwave signal unique to the individual) in a single step by performing a single mental task. Additionally, the robustness of this method against impersonation attacks was demonstrated, including conditions where the attacker may have learned the target's secret thought and/or secret task.

In the present proposal, we will undertake, to the best of our knowledge, the first ever study of one-step three-factor authentication. In computer security, authenticators are classified into three types: knowledge factors (e.g., passwords and PINs), possession factors (e.g., physical tokens, ATM cards), and inherence factors (e.g., fingerprints and other biometrics). Because three-factor authentication (3FA) requires the user to submit one distinct instance of each type of authenticator, it represents the strongest level of authentication security possible.

We propose the use of custom-fit Ear EEG technology as the platform for investigating the feasibility, performance, and usability of one-step three-factor authentication. In addition to the same knowledge factor and inherence factor as in previous work, the user can submit in the same step the possession factor in the form of the EEG-sensing ear-piece(s) that are custom-fitted to and worn in their ear. These earpieces can serve as physical tokens in the same way as bank ATM cards and wearable hardware tokens. Furthermore, because the earpieces are custom-fitted to each individual, they will likely not be able to produce good electrical impedances when worn by a different individual.

2 Related work

The use of EEG as a biometric signal for user authentication has a short history. In 2005, Thorpe et al. motivate and outline the design of a passthoughts system, where, rather than typing a password, users authenticate by thinking of a passthought. Since 2002, a number of independent groups have achieved 99- 100\achieved using a consumer-grade single-channel sensor. In particular, the lack of signal diversity from multiple EEG channels can be overcome by allowing the users to choose their own personalized passthoughts (e.g., sing their favorite song in their head). There are two significant consequences

of this result. First, the passthoughts approach is no longer constrained by the high cost ($>$ \$10,000 USD) and low usability (gel-based electrodes; aesthetic challenges of an EEG cap) of medical-grade multi-channel devices. Second, because users can choose and easily change their secret mental task, this approach can support one-step two- factor authentication via the simultaneous presentation of the inherence factor (brainwave signatures due to the unique folding structures of the cortex) and the knowledge factor (the secret mental task).

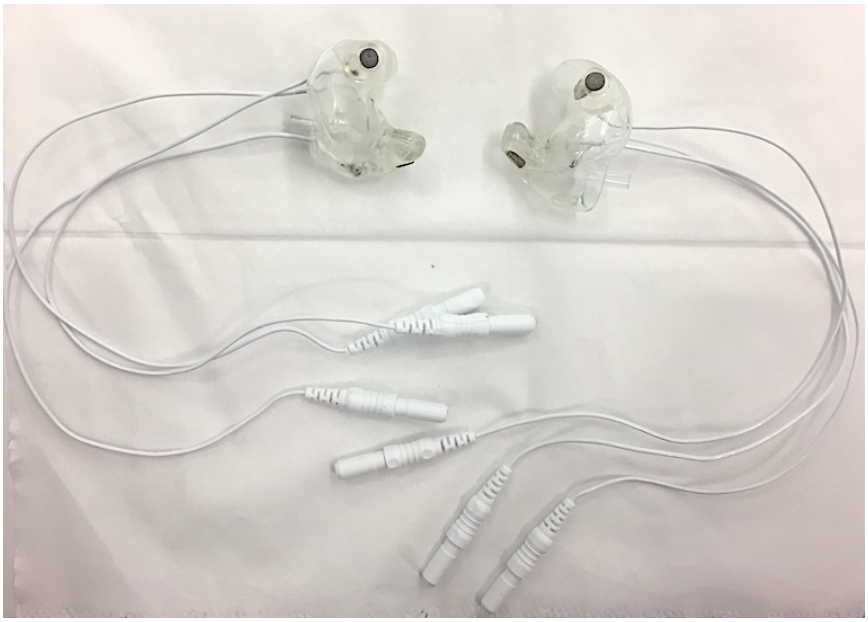

Figure 1: Pair of custom-fit earpieces with 3 embedded electrodes each located at the helix and front-facing and back-facing within the ear canal.

Research in in-ear EEG is only several years old. Nonetheless, the concept has attracted a lot of attention because of the discreetness factor of in-ear EEG over traditional scalp-based EEG. A research team at the Imperial College London and Aarhus University published a landmark paper in 2011 that introduced the concept of in-ear EEG, demonstrating for the first time the feasibility of recording brainwave signals from within the ear canal. Follow-up work from the same group demonstrated its ability to produce signal-to-noise ratios comparable to those from conventional EEG electrode placements, robustness to common sources of artifacts, and use in a brain-computer interface (BCI) system based on auditory evoked potentials and

visual evoked potentials. Citation to our pst work was the first to merge these two streams of work, using in-ear EEG signals for user authentication with a consumer-grade device. United Sciences is currently developing a consumer hearable called The Aware that will measure EEG from the ear. Behavioral authentication methods such as keystroke dynamics and speaker authentication can be categorized as one-step two-factor authentication schemes. In both cases, the knowledge factor (password or passphrase) and inherence factor (typing rhythm or speaker's voice) are employed. In contrast, the Nymi band supports one-step two-factor authentication via the inherence factor (cardiac rhythm that is supposed to be unique to each individual) and the possession factor (the wearing of the band on the wrist). However, as far as we know, no one has proposed or demonstrated a one-step three-factor authentication scheme.

3 Methods

3.1 TODO Manufacturing, materials

3.2 Subjects

3.3 TODO Tasks

Explain stuff around tasks

Task	**Description**
Breathe	Relaxed breathing with eyes closed.
Breathe - Open	Relaxed breathing with eyes open.
Sport	Sport-related motor imagery of participant's choice.
Song	Imagining a song of participant's choice playing.
Song - Open	Imagining a song with eyes open.
Speech	Imagining a phrase of participant's choice being spoken.
Listen	Tone & Listening to a continuous tone.
Listen - ASSR	Listening to noise modulated at 40 Hz.
Face	Imagining a person's face of participant's choice.
Sequence	On timed cues, imagine a face, a number, and a word.

Table 1: Set of tasks proposed for authentication with descriptions.

Task	External stimuli?	Knowledge factor ?	Eyes?	Imagery?
Breathe	No	No	Closed	None
Breathe - open	No	No	Open	None
Sport	No	Yes	Closed	Motor
Song	No	Yes	Closed	Aural
Song - open	No	Yes	Open	Aural
Speech	No	Yes	Closed	Aural
Listen - Tone	Yes	No	Closed	None
Listen - ASSR	Yes	No	Closed	None
Face	No	Yes	Closed	Visual
Sequence	Yes	Yes	Open	Visual

Table 2: Properties of authentication tasks. We selected tasks with a variety of different properteries, but preferred tasks that did not require external stimuli, as the need to present such stimuli at authentication time could present challenges for usability, and user security.

3.4 Protocol

Our initial participants were recruited from a nearby university and scheduled for ear molding and impedance checking sessions. Finally, the data collection visit was scheduled and took approximately 90 minutes for set up and experiment execution. The OpenBCI system we used allows for 8 channels of simultaneous recording, along with separate ground and reference channels. Data was initially collected with the ground placed at the center of the forehead, and using the left mastoid as reference, though we can easily re-reference to another channel by subtracting a desired channel (such as right mastoid). Each earpiece (shown in the image below) contain three channels: one placed on the helix, and two inside the canal - one front-facing and the other back-facing. The remaining two channels were placed on the right mastoid for later re-referencing, and at approximately Fp1 (on the forehead above the left eye) for validating the data collected in the ears against a scalp-based measure. Before beginning the experiment, the data from all channels was visualized and participants were asked to blink and clench their jaws to confirm visibly that all channels were active and properly connected.

During the experiment, participants were seated in a comfortable position in a quiet room facing a laptop screen on which the instructions and stimuli were presented using PsychoPy. Each task was completed once in sets five trials each, and then each was completed again for another five trials. Each

trial was 10 seconds in length, for a total of 10 trials and 100 seconds of data collected per task. The instructions were read aloud to the participant by the experimenter, and the experiment was advanced using a pointer held in the participant's lap to minimize motion artifacts in the data. The experimenter also recorded the participant's chosen secrets for the sport, song, face, speech, and sequence tasks and reminded the participant of these for the second set of trials.

4 Analysis

4.1 Validating the data

In this section, we establish that the data we collected were EEG signals with relatively low noise. Using the pilot data from two participants, we were able to confirm the custom-fit earpieces are able to collect EEG data using three tests: good impedances measured for the ear electrodes, alpha-band activity attenuation when a participant's eyes were open versus closed, and the presence of a significant ASSR signal.

The recorded impedances of the earpiece electrodes were less than 5 kOhms except one, a benchmark used widely in previous ear EEG work. The left helix electrode of one participant was measured at 9 kOhms, and generally the helix impedances for both participants were higher than their ear canal counterparts. We expected this result, given that the helix electrode relies on quality of the earpiece's fit outside the ear for good contact, and is not as securely and tightly placed as the electrodes within the ear canal. Nonetheless, the data from all electrodes were tested in the remaining two data quality tests.

For the alpha-attenuation test, data from the "Breathe" task was compared with that of the "Breathe - Open" task. It is a well- known feature of EEG data that activity in the alpha-band (approximately 8-12 Hz range) increases when the eyes are closed compared with a similar state with eyes open. For both of our pilot participants this attenuation is clearly visible even in just a single trial's data. To further validate, we also performed this calculation on the data collected from the Fp1 electrode and see the effect clearly here as well. It is important to note that the left ear results are reported using the right mastoid as reference, and the right ear results in turn using the left mastoid as reference. When using the same side mastoid for reference the effect is not visible, though it may be if we average across many trials. This is not surprising, as the further a reference electrode is from the active channel the less "real" signal is being subtracted from the

active channel. This has important design implications for eventual real-world deployment of this authentication method however, as it will likely require pieces worn on or around both ears to properly function, and not just one. The figures below show the alpha attenuation in the left and right ear channels, as well as Fp1.

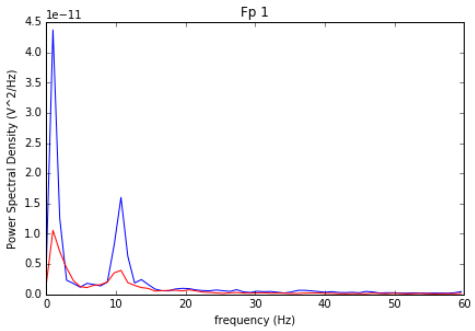

Figure 2: Alpha-attenuation (8-12 Hz range) in Fp1 channel, referenced at left mastoid, for comparison to ear channels. Red indicates breathing data with eyes open, blue indicates the same task with eyes closed.

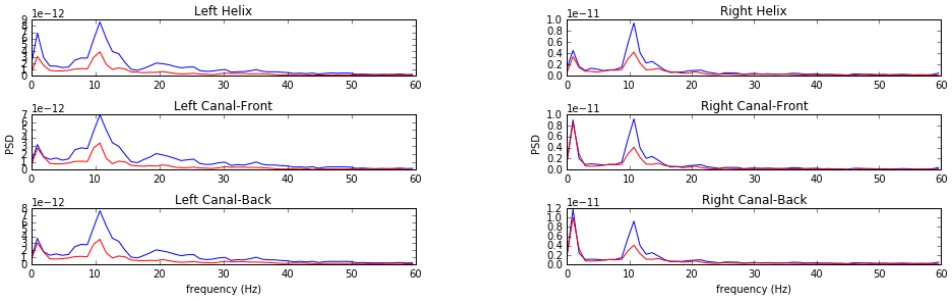

Figure 3: Alpha-attenuation (8-12 Hz range) in left and right ear canal channels, referenced at opposite mastoids respectfully. Red indicates breathing data with eyes open, blue indicates the same task with eyes closed.

Finally, for the ASSR test we calculated power spectra for data from the "Listen - ASSR" task. The audio stimulus used for this task is modulated at 40 Hz, which should, in turn, produce an EEG response visible in the data at 40 Hz. Strangely, in our tests we do see an ASSR spike but it is located around 74 Hz instead. While this has us somewhat perplexed about our stimulus, the purpose of this test was to ensure that the response seen in

the ear channels matched the response seen from the Fp1 recordings, which is evident comparing the figures below.

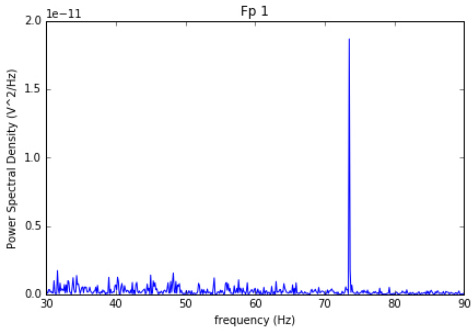

Figure 4: Power spectrum for data collected from the Fp1 channel during 40 Hz ASSR stimulus. An ASSR spike is clearly visible, though not at 40 Hz where it was expected.

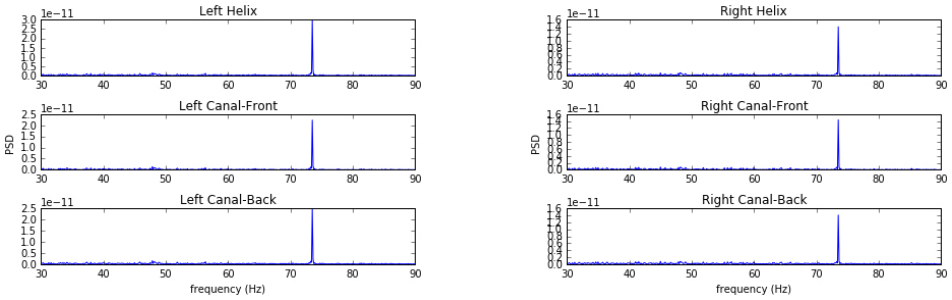

Figure 5: Power spectra for data collected from the earpiece channels during 40 Hz ASSR stimulus. Again, the spike is clearly visible though not at 40 Hz, however it does match the activity measured at Fp1.

4.2 TODO Classification

4.3 TODO Simulating an imposter attack

5 Results

5.1 TODO Combinations of electrodes

Figure: Plot of FAR/FRR by electrode combination, XGBoost and LinearSVC.

5.2 TODO Left-ear authentication

Our main result:

Table: FAR/FRR Between-subjects results by participant (avg. all tasks? Best task?)

Our attempt to substantiate that we have both inherence and knowledge factors:

Table: original strategy, within-subjects, within-tasks strategy; where each of those headings is subdivided into mean FAR, mean FRR (across all subjects and tasks)

5.3 TODO Imposter attack

5.4 TODO Usability

Quantitative and qualitative data, where appropriate

6 TODO Discussion

1. Apparent feasibility of single earpiece
2. Balancing between FAR & FRR, improvements over previous work
3. Notable patterns: best task breathe across participants; each feature vector represents very little time (500ms)
4. Counter to expectations: referencing same side appears to be an improvement vs. across the head; use of conductive gel resulting in ability to achieve good impedances on others' earpieces; FP1 not performing as well as expected.

7 TODO Conclusion & Future Work:

- How will this system change with more users? How will this system change with more diverse data?
  - EEG stability
  - Also breakdown/malfunction
  - Address with? Ambulatory settings, Exercise, alcohol, caffeine, etc.
- How "hackable" is a passthought?

  - Point from NSPW draft
  - Address with? Statistical analysis & hacking existing classifiers

- UX improvements/innovations?
  - Dry electrodes?
  - Closed-loop system?

Closed-loop BCI system could help us understand how learning effects on the human side might impact authentication performance, as the human and machine co-adapt during multiple authentication attempts.