One-Step, Three-Factor Authentication With Custom-Fit, In-Ear EEG

First Name, Second Name, Third Name
First Institution

Second Name
Second Institution

Abstract

In this paper, we present a system that provides all three factors of authentication (knowledge, possession, and inherence) in a single step by using brain-based authentication via custom-fit, in-ear electroencephalography (EEG). We demonstrate its potential by collecting electroencephalography (EEG) data from seven participants using manufactured custom-fit earpieces with embedded electrodes. Across all participants, we achieve mean 0% false acceptance and 0.017% false rejection rates with data from only one earpiece with three electrodes. Furthermore, we find a 0% false acceptance rate in a preliminary simulation of an impersonation attack. We also report some positive usability perspectives from our participants and discuss constructive directions for future work. Our results indicate that in-ear EEG could provide a discreet, convenient, and usable method for secure one-step, three-factor authentication.

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, faces many challenges. Major industry players such as Google and Facebook have strongly encouraged their users to adopt two-factor authentication (2FA). However, submitting two different authenticators in two separate steps has frustrated wide adoption due to its additional hassle to users. The Apple iPhone, for instance, already supports device unlock using either a user-selected passcode or a fingerprint. The device could very well 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 cost of two-step verification. In this study we 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). By taking advantage of a physical token in the form of personalized earpieces, the uniqueness of an individual's brainwaves, and a choice of mental task to use as one's passthoughts, we seek to achieve all three factors of authentication in a single step by the user.

We find that we can achieve low false acceptance rates (FAR) and false rejection rates (FRR) with a single, three-electrode earpiece. Interestingly, we found that performance in our protocol improves in the ear compared to a single electrode placed more traditionally on the scalp. Additionally, we find that passthoughts are not able to be spoofed by imposters, either from within the data set or outside of it, even when the imposters had a user's earpiece that fit their ear and knew their chosen passthoughts. We discuss the benefits of passthoughts for usable authentication, and raise questions for future pursuit about how and why passthoughts work as well as they do.

2 Related Work

2.1 Passthoughts Authentication

The use of EEG as a biometric signal for user authentication has a short history. In 2005, Thorpe et al. motivated and outlined the design of a passthoughts system

[27]. Since 2002, a number of independent groups have achieved 99- 100% authentication accuracy using multi-channel sensors placed on the scalp [25, 16, 23, 2]. In 2013, one group showed that 99% authentication accuracy can also be achieved using a consumer-grade single-channel sensor [6]. 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 a full 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) [5].

By employing scalp-based consumer-grade electroencephalography (EEG), it was demonstrated in a 2014 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 [5]. 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 [10].

Following this, we investigate custom-fit in-ear EEG technology as the platform for investigating the feasibility, performance, and usability of one-step three-factor authentication worn unobtrusively. The system we propose and test here uses the choice of a mental task or "passthought" to perform as knowledge (factor one), the uniqueness of an individual's brain activity as measured by EEG as inherence (factor two), and the physical token of custom-fit earpieces, which could easily contain a hardware key-pair, as a possession factor (factor 3). 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. The ability to utilize all three of these security factors in a single step by performing a mental task of a few seconds is a promising in pursuit of extremely strong security while maintaining a low amount of effort and obtrusiveness to the user.

2.2 In-Ear EEG

Even consumer-grade headsets can be uncomfortable to wear, and are awkwardly visible to outside observers. Sensors placed around the ear however, present a more discreet, comfortable location for an EEG sensor, as many people already wear technology like earbuds in day-to-day life.

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 [15]. 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 [14, 12, 11]. United Sciences is currently developing a consumer "hearable" (in-ear wearable) called The Aware, which will measure EEG from the ear, among other biometrics [28].

[7] was the first to merge in-ear EEG with passthought authentication, using a modified consumer grade EEG device with a single electrode, achieving approximately 80% authentication accuracy.

2.3 One-Step, Multi-Factor Authentication

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 [20]. 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) [21]. However, as far as we know, no one has proposed or demonstrated a one-step three-factor authentication scheme, in which possession of a unique device also serves to authenticate the user. In this paper, we introduce custom-built EEG devices, incorporating an added possession factor to the already one-step two-factor authentication provided by passthoughts.

2.4 Usable Authentication

Typical authentication protocols are often susceptible to a so-called *rubber-hose attack*, in which users are coerced into giving up their chosen secret (e.g. alphanumeric password), biometric, or unique token, voluntarily or otherwise [3, 17]. This attack is particularly effective against protocols that rely only on inherence factors, as inherent traits such as fingerprints are difficult to change without costly repercussions [26]. One defense against such an attack is *tacit authentication*, in which the user does not know exactly how s/he performs the authenticating action and thus cannot fully give it away even under duress.

Past work has exploited tacit skills (skills we know how to do, but cannot readily explain our method for doing, e.g. riding a bike or walking [3]. In practice, these skills require time to learn, and the fact that they are performed visibly could open up opportunities for recording and replay attacks.

Our work explores a different solution to rubber-hose attacks: a thought, which is secret (and thus changeable), but has a particular expression unique to an individual, the performance of which cannot be described (and thus cannot be coerced). Furthermore, the performance of the chosen thought is largely invisible to outside observers, ensuring the actual authentication is impervious to shoulder-surfing.

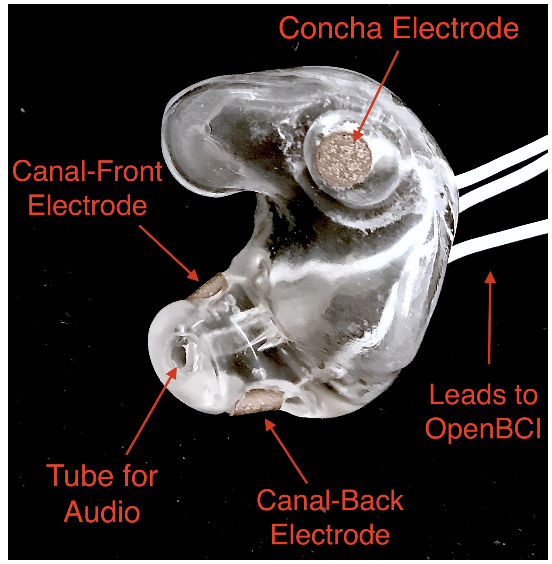

Figure 1: Labeled photo of one of our manufactured custom-fit earpieces with 3 embedded electrodes located in the concha, front-facing (anterior) in the ear canal, and back-facing (posterior) in the ear canal.

3 Methods

3.1 Study Overview

7 male participants (P1-P7), 5 students and 2 non-students, completed our study protocol that was approved by our local Institutional Review Board. Three study visits took place per participant, in the first the 3D molds of participants' ears to use in creating the earpieces were obtained, the second was a fit and electrical impedance check once earpieces were manufactured, and the third to collect data using the earpieces while participants performed a set mental tasks to be used in authentication analysis. Informed consent was obtained prior to study procedures. The third study visit consisted of participants completing a short demographics questionnaire, a set up period with the OpenBCI system and earpieces including a second impedance check, the performance of 9 mental tasks presented on a laptop, and finally a post-experiment questionnaire. Approximately two weeks after the third study visit, a subset of participants reported via e-mail whether or not they remembered the passthoughts they chose and performed during the third visit.

3.2 Earpiece Design and Manufacturing

To produce custom ear impressions during the first study visit, we cleaned subjects' ears and injected silicon into the ear canals. A cotton ball with a string attached is placed into the ear canal first. When the silicon dries after a few minutes, the string is pulled to remove the impression from the ear canal. This impression is then scanned with a 3D scanner and the resulting scan modified based on some heuristics to achieve a comfortable fit and to ensure the intended electrode sites will make good contact with the skin. Channels are created in the 3D model to allow wire leads and associated EEG electrodes as well as a plastic tube to deliver audio. This 3D model is then sent to a 3D printer. Following this wires, leads, and associated AgCl electrodes are installed.

The positions of the earpiece electrodes were simplified from those described in [19]. We reduced the number of canal electrodes in order to prevent electrical bridging and positioned them approximately 180 degrees apart in the canal (posterior/back and anterior/front locations in the canal). We also reduced the number of electrodes in the concha to one. An example of one of the manufactured earpieces is shown in Figure 1.

3.3 Mental Tasks

We used a set of mental tasks based on findings in related work regarding the relative strengths of different tasks in authentication accuracy and usability as reported by participants. Furthermore, given the in-ear placement of the electrodes and therefore the proximity to the temporal lobes containing the auditory cortex, we tested several novel authentication tasks based specifically on aural imagery or stimuli. The 9 authentication tasks and their attributes are listed in Table 1. Our strategy was to select tasks that captured a diversity of possibilities across the dimensions of external stimuli, involving a personal secret, eyes open or closed (due to known significant effects on EEG), and different types of mental imagery.

3.4 Data Collection Protocol

The data collection visit took approximately 90 minutes for set up and experiment execution. All collection sites were cleaned with ethanol prior to electrode placement, and a small amount of conductive gel was used on each electrode. For EEG recording we used OpenBCI [18], an open-source biosensing system to maintain an overall low cost for our setup. OpenBCI costs about 600 USD, and thus is an affordable alternative to medical-grade EEG systems that can cost tens of thousands of dollars. Recent work has demonstrated the robustness of OpenBCI compared to an industry standard medical-grade EEG system, particularly for non-medical use cases such as ours [8]. The OpenBCI system we used allows for 8 channels of simultaneous recording, along with separate ground and reference channels. Data was collected with the ground placed at the center of the forehead, approximately AFz according to the 10-20 International Standard for Electrode Placement (ISEP), and using the left mastoid as reference. Notably, when examining data from the right earpiece, we re-referenced to the right mastoid channel so that our results reflect data from a single ear. Each earpiece (shown in Figure 1) contains three channels, for the remaining two channels AgCl ring electrodes were placed on the right mastoid for later re-referencing, and at approximately Fp1 (left frontal lobe region, above the left eye in accordance with the ISEP) for validating the data collected in the ears against a common scalp-based placement. Before beginning the experiment, the data from each channel was visually inspected using the OpenBCI interface and participants were asked to blink and clench their jaws to confirm that all channels were active and properly connected. Audio stimuli were delivered through small tubes in the earpieces opening into the ear canal.

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 [24]. 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.

After completing the experiment, a subset of participants completed a usability questionnaire in which they were asked to rate their ease of performing, level of engagement, perceived repeatability, and likeliness of using each task. The questionnaire also asked participants to rank the tasks overall from most to least favorite, as well as several open response questions regarding potential use cases of in-ear EEG and this method of authentication, level of comfort wearing the earpieces, and any other comments they chose to provide.

4 Analysis

4.1 Data Validation

In this section, we establish that the data we collected were of a neural origin, and had relatively little noise. We were able to confirm the custom-fit earpieces are able to collect EEG data via two metrics: good impedances measured for the ear electrodes, and alpha-band EEG activity attenuation when a participant's eyes were open versus closed.

The first quality check was examining the electrical impedances achieved for the ear pieces as a low impedance (¡10 kOhm) is best for obtaining quality EEG signals. Table 2 below summarizes the impedances across the seven participants' six ear channels. With the exception of a few channels in select participants, impedances achieved were overall good. Most of the recorded impedances of the earpiece electrodes were less than 5 kΩ, a benchmark used widely in previous ear EEG work, and all except two were less than 10 kΩ. 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 our 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 to compare. Figure 2 shows the alpha attenuation in the left ear channels, as well as Fp1 of one participant as an example. We see the same effect in the right ear channels.

4.2 Classification

We analyzed the EEG signals collected during the tasks using a support vector classifier (SVC). Since past work has shown that classification tasks in EEG-based BCI

Task	Description	Stimuli?	Secret?	Eyes	Imagery
Breathe	Relaxed breathing with eyes closed	No	No	Closed	None
Breathe - Open	Relaxed breathing with eyes open	No	No	Open	None
Sport	Imagine attempting a chosen physical activity	No	Yes	Closed	Motor
Song	Imagine hearing a song	No	Yes	Closed	Aural
Song - Open	Song task, with eyes open	No	Yes	Open	Aural
Speech	Imagine a chosen spoken phrase	No	Yes	Closed	Aural
Listen	Listen to noise modulated at 40 Hz	Yes	No	Closed	None
Face	Imagine a chosen person's face	No	Yes	Closed	Visual
Sequence	Imagine a chosen face, number, and word on timed cues	Yes	Yes	Open	Visual

Table 1: Properties of authentication tasks. We selected tasks with a variety of different properties, 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.

	Impedances [kΩ]					
	Left ear			Right ear		
P	C	F	B	C	F	B
1	4	4	4	<1	4	3
2	9	5	4	3	4	4
3	4	5	4	9	6	9
4	4	5	4	3	16	9
5	9	20	7	3	7	9
6	5	8	2	1	1	9
7	2	9	8	7	5	6

Table 2: Electrical impedances measured for earpiece electrodes, for concha (C), front (F) and back (B).

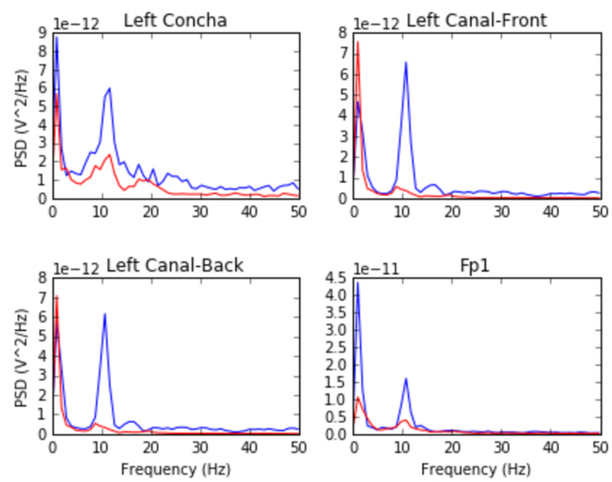

Figure 2: Alpha-attenuation (8-12 Hz range) in left ear channels compared against the Fp1 channel, referenced at left mastoid. Red indicates breathing data with eyes open, blue indicates the same task with eyes closed.

are linear [9], we used XGBoost, a tool for logistic linear classification [4]. Compared to other linear classifiers, XGBoost uses gradient boosting; in which an algorithm generates an ensemble (in this case, a decision tree) of weak linear classifiers that minimizes a given loss function. Gradient boosting gives better results in linear classification problems, without our needing to manually tune classifier hyperparameters.

To produce feature vectors, we took slices of 100 raw values from each electrode (about 500ms of data), and performed a fourier transform to produce power spectra for each electrode during that slice. We concatenated all electrode power spectra together, and performed principal component analysis on all concatenated vectors such that the resulting vectors described 95% of the variance in the full power spectrum data. For each task, for each participant, 100 seconds of data were collected in total across 10 trials of 10 seconds each, resulting in 200 samples per participant, per task, following this preprocessing.

We trained the classifier using a balanced sample of positive and negative examples, where positive examples were from the target participant and target task, and negative examples were randomly selected tasks from any participant besides the target participant. From this corpus of positive and negative samples, we withheld one third of data for testing. The remaining training set was fed into a XGBoost's cross-validation method, which we set to iteratively tweak parameters over a maximum of fifty rounds of cross-validation to minimize loss. After cross-validation, the updated classifier (with parameters applied) predicted labels on each sample in the test set, and we calculated FAR and FRR on its results.

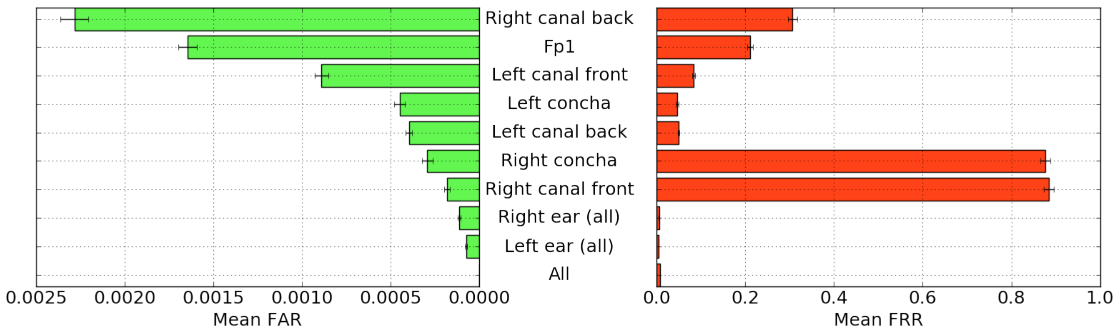

Figure 3: FAR by electrode configuration. All electrodes combined achieves a perfect score. We achieve the next best scores using data from the left ear only.

5 Results

5.1 Combinations of electrodes

For each configuration of electrodes, we calculated the mean FAR and FRR across all participants using each task as the passthought (Figure 3). Incorporating all electrodes' data results in a perfect score for all tasks. Using data from all left-ear electrodes achieves the next lowest FAR, followed by all right ear electrodes. Notably, no single electrode from the left or right ear performs as well as the aggregate left and right ear conditions.

Counter to our expectations, Fp1 does not perform as well as most ear electrodes, though overall these reported rates are far less than 1%. Further, while FRR seemed to correlate roughly with FAR for most electrodes, the right concha and right canal front electrodes achieved extremely high FRRs, while their FARs were among the lowest.

Our results indicate acceptable accuracy using electrodes on the left ear alone. This corresponds to our original scenario, in which the device could be worn like an earbud (ideally, only one earbud would need sensors). As such, we focus on results from the left ear alone in our following analyses.

5.2 Authentication Results

In the previous section, we trained and tested a passthought classifier with each task as the passthought, for all participants. Our analyses revealed the choice between left and right ear to have little effect on the results and this enables us to postulate around a more usable device using sensors only around the left ear. Focusing on the left ear, we filter our results for the best-performing tasks. We rank tasks by lowest FAR and, given a tie, the lowest FRR (Table 3).

All best-performing tasks in our best-case set achieved perfect FAR and FRRs, with the exception of P5, whose best-performing task (*breathe*) had a nonzero FRR. *Breathe* appeared as the best task across all participants, except P1. Given our training strategy, these results indicate that a given person's *breathe* task is distinguishable not only among other tasks, but among *breathe* tasks from other participants. This task performed about as well as its open-eyes counterpart (Figure 4), as did *song - open* and *sport* (though, interestingly, *song* with eyes closed performed less well).

P	FAR	FRR	Task
1	0.000	0.000	Listen
2	0.000	0.000	Breathe
3	0.000	0.000	Breathe
4	0.000	0.000	Breathe
5	0.000	0.012	Breathe
6	0.000	0.000	Breathe
7	0.000	0.000	Breathe

Table 3: Best-performing passthought, with FAR and FRR, for each participant (P), using data from the left ear.

These results establish good performance in our original training strategy, in which we count as negative examples recordings from the wrong participant performing any task. For comparison, we try two additional training strategies: one in which negative examples are the correct task recorded from the wrong participant (within-tasks), and one in which negative examples are the incorrect task recorded from the correct participant (within-participants).

Overall, our original training strategy achieves the lowest FAR (Table 4). Within-tasks FAR ten times higher, and within-participants FAR is one hundred times higher, though all scenarios still less than 1%. However, FRR is *lower* in the within-tasks training strategy than in our original strategy's FRR. Within-participants again results in the highest FRR.

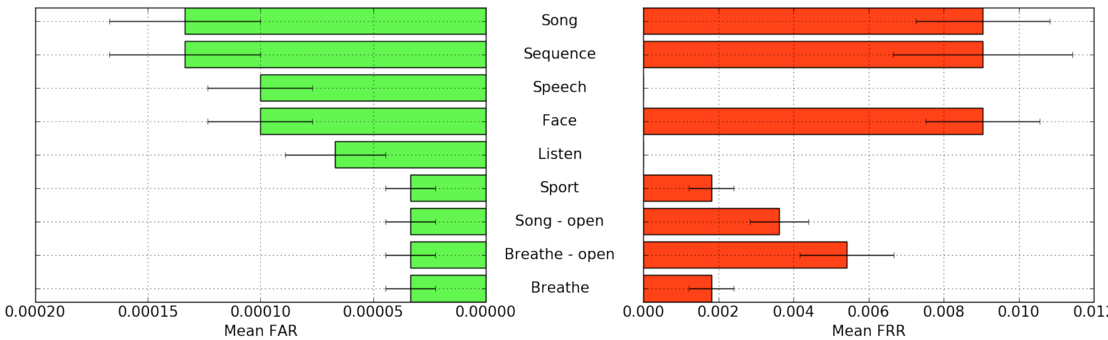

Figure 4: FAR by task, across all subjects, using data from the left ear only.

	FAR	**FRR**
Original	0.000074	0.004424
Within-tasks	0.000724	0.001522
Within-participants	0.002523	0.039702

Table 4: Mean FAR and FRR for all participants and passthoughts across three different training strategies.

5.3 Usability

A subset of four participants completed our usability questionnaire. This questionnaire asked them to rank each of the mental tasks on 7-point likert-type scales on ease of use, level of engagement, perceived repeatability, and likeliness to use in a real-world authentication setting. The *breathe* and *listen* (μ=6.75) tasks were ranked easiest to use, while the *sequence* (μ=2.25) and *face* (μ=2.75) tasks were ranked the most difficult. *Sequence* was rated highly in engagement however (μ=5), as was *song* (μ=5), while *breathe-open* and *listen* were ranked least engaging (μ=2.25). *Breathe* (μ=7) and *listen* (μ=6.75) were ranked highest in repeatability, with *sequence* (μ=2.5) along with *face* and *sport* (μ=3) ranked least repeatable. Finally in terms of likeliness of use for authentication, *song-open* (μ=5) and *sequence* (μ=4.25) were rated highest, though modestly, while *breathe* (μ=2.75) and *listen* (μ=3) were rated least likely to use.

In addition to these rating scales we asked participants to rank the tasks from most (1) to least (9) favorite overall. The *song - open* task ranked highest among favorites (μ=4.25) followed by a tie between *breathe - open*, *song*, and *speech* (μ=4.75). In line with some of the results above, *sequence* (μ=7.75) and *face* (μ=6.75) were rated as least favorites.

In addition to the scales and rankings, we included in our questionnaire a few open response questions to ascertain attitudes about the use cases for in-ear EEG and passthoughts, and the comfort of wearing an in-ear EEG device in everyday life. Participants first read the prompt, "Imagine a commercially available wireless earbud product is now available based on this technology that you've just experienced. It requires minimal effort for you to put on and wear.", and were asked about use cases for in-ear EEG and passthoughts. Responses about in-ear EEG expectedly included authentication for unlocking a phone or computer and building access, but also aspects of self-improvement such as P4's response "Help people increase focus and productivity". P5 and P6 also indicated a use for measuring engagement with media like movies and music, and relatedly P4 wrote "music playback optimized for current mental state and feelings". In terms of comfort wearing such a device, participants generally responded they would be comfortable, though P5 and P6 stipulated only when they would otherwise be wearing something like earphones in their ears already. In response to an "any other comments" prompt, notably three participants pointed out the mental imagery of a face was difficult for them and some concerns about their ability to repeat tasks in the same exact way each time.

A final component of usability we measured was the ability of the participants to recall their specific chosen passthoughts for the *song*, *sport*, *speech*, *face*, and *sequence* tasks. Participants were contacted approximately two weeks after their data collection study visit and were prompted with these categories and asked to respond with what they remembered their choices being. As evidenced by their responses, all participants were able to recall all of their chosen secrets, with the exception of one participant who incorrectly remembered their chosen word for the *sequence* task.

6 Imposter Attack

While our left ear results establish that passthoughts achieve low FAR and FRR when tested against other participants' passthoughts, we do not know how robust passthoughts are against a spoofing attack, in which both a participant's custom-fit electrode, and details of that participant's chosen passthought, are leaked and used by an imposter.

The first aspect of this scenario we tested was the ability of an imposter to wear an earpiece acquired from someone else and achieve viable impedance values for EEG collection based on the fit of the pieces in their ears. P1 tried on each of the other participants' earpieces, which were able to at least somewhat fit in P1's ears. The impedances of P1 wearing other participants' earpieces were then recorded and are listed in Table 5 below. While some are a better fit than others, overall they are higher than those achieved by the pieces' intended owners themselves.

Impedances [kΩ]

	Left ear			**Right ear**		
P	**C**	**F**	**B**	**C**	**F**	**B**
2	34.1	10.2	12.8	27.8	16.0	16.3
3	21.1	20.9	19.0	13.5	11.3	19.5
4	14.1	11.9	9.7	11.0	11.1	13.3
5	17.2	21.9	10.3	32.6	12.5	11.6
6	18.7	10.0	8.4	14.8	11.5	8.9
7	91.5	>1000	21.5	33.5	26.4	31.0

Table 5: Electrical impedances achieved with P1 wearing each other participant's (P) custom-fitted earpieces, for concha (C), front (F) and back (B).

To explore the scenario of an imposter attempting to gain access, we chose the worst case participant, P6, whose earpieces P1 had the lowest impedances while wearing. We collected data using the same data collection protocol, but had P1 refer to P6's report of chosen passsthoughts. P1 performed each of P6's passthoughts (simulating an "inside imposter"). Following the same classification and preprocessing steps, we generated 200 samples per task for our imposters, using data from all left ear electrodes.

Since every participant has one classifier per task (for which that task is the passthought), we are able to make 200 spoofed attempts with the correct passthought on each of P6's classifiers (Table 6). We find no successful spoof attempts for tasks with a chosen secret (e.g., *song* or *face*). However, we also do not find any successful spoof attacks for tasks with no chosen secret (e.g., *breathe*). In fact, in all 1,800 spoof attempts (200 attempts for each of the 9 classifiers), we do not find a single successful attack on any of P6's classifiers.

However, since this participant's data appeared in the initial pool, the classifier may have been trained on his or her recordings as negative examples. To explore the efficacy of an outsider spoofing recordings, we repeated the same protocol with an individual who did not appear in our initial set of participants (an "outside imposter," Table 6). Again, find zero successful authentication attempts.

Task	FAR (Insider)	FAR (Outsider)
Breathe	0.0	0.0
Breathe - Open	0.0	0.0
Sport	0.0	0.0
Song	0.0	0.0
Song - Open	0.0	0.0
Speech	0.0	0.0
Listen	0.0	0.0
Face	0.0	0.0
Sequence	0.0	0.0

Table 6: False acceptance rate for spoofed versions of P6's passthoughts, performed by an inside imposter (P1 from the original participant pool) and an outside imposter (not from the original participant pool).

7 Discussion

Our findings demonstrate the apparent feasibility of a single earpiece, achieving good results with only three electrodes and a reference, all on or around the left ear. FARs and FRRs are very low across all participants and tasks, with FARs overall lower than FRRs, a desirable pattern in terms of authenticating access to potentially sensitive information. Participants' best-performing passthoughts typically see no errors in our training. Furthermore, no spoofed attacks were successful in our cursory analysis.

This study was conducted with a small, relatively homogeneous sample of participants. We feel that more participants from a more diverse pool would greatly improve our understanding and interpretation of the capabilities of this technology. This does not lessen the importance of this work however, as this sample size is comparable to that of previous scalp-based EEG passthoughts work[2, 16, 23, 22, 25, 6], the only other in-ear EEG passthoughts study we are aware of [7] (notably a generic fit system was used here), and other custom-fit in-ear EEG research [13]. The fitting and manufacturing of custom-fit earpieces was the main limitation to increasing our sample size, and may very well pose a limitation in proliferation and adoption of such a technology. Recently however, there have been developments in at-home kits for creating one's own custom-fitted earpieces [29] that could help overcome this barrier.

In our analysis, some notable patterns emerged. First, *breathe* tended to be the best-performing task among participants. Classifiers overall distinguished the *breathe* task even compared to *breathe* tasks from other participants, implying that the task is expressed differently for each participant, i.e. that this task has an inherence factor sufficient for authentication, even though the task does not have an explicit secondary knowledge factor as in *song*, for example. Second, we were able to achieve good results by generating feature vectors based on only 500ms (300 voltage readings across the three electrodes). This short timespan is somewhat surprising, given that some tasks (like songs) presumably rely on changes or patterns over a longer period of time.

Furthermore, likely due to the use of conductive gel, low impedances are still achievable using other participants' custom-fit earpieces, despite the uniqueness of ear canal shapes between individuals [1]. Nevertheless, classifiers appear to resists spoofing attacks, indicating that task-related signals are unique to individuals. In terms of establishing a possession factor, the custom-fit earpiecs could easily include a hardware keypair to sign authentication attempts in a three-factor, one-step scheme.

The powerful interactions between inherence and knowledge emerged in our spoofing attack. Although our target participant documented their chosen passthought, the spoofers found ambiguity in how these passthoughts could be expressed. For the *face* task, the spoofers did not know the precise friend the original participant had chosen. For the *song* and *song - open* tasks, though the song was known, the spoofers did not know what part of the song the original participant had imagined, or how it was imagined (humming, imagining a full performance, melody, vocals, etc). This experience sheds light on the highly individual nature of passthoughts, and provides a positive indication that there may be some intrinsic difficulty in spoofing attempts of passthoughts.

Finally, performance on Fp1 was not as high as performance in the ear, despite Fp1's popularity in past work on passthoughts [6]. This could be explained by the greater number of electrodes in the ear (compared to just one on Fp1). Additionally, Fp1 is best poised to pick up on frontal lobe activity (e..g, concentration), but our tasks did not generally involve frontal lobe activity; in fact, a good number of them involved audio, which we would expect to be better observed near the auditory cortex at the ears. Future work should continue to investigate what sorts of mental tasks lend themselves to in-ear recording.

8 Future Work

One primary question surrounds how our passthoughts system performance will change with a greater number of users, and with more diverse data. Our system specifically trains on negative examples of incorrect users; we do not yet know how this approach will scale. At the same time, we must investigate the stability of EEG readings for a passthought are over time to establish long-term usability. We must also collect EEG data from the variety of different user states: ambulatory settings, during physical exertion or exercise, under the influence of caffeine or alcohol, etc.

Another important question surrounds how passthoughts might be cracked. Generally, we do not understand how an individual's passthought is drawn from the distribution of EEG signals that an individual produces throughout the day. Given a large enough corpus of EEG data, are some passthoughts as easy to guess as *password1234* is for passwords? Future work should perform statistical analysis on passthoughts, such as clustering (perhaps with t-SNE) to better understand the space of possible passthoughts. This work will allow us simulate cracking attempts, and to develop empirically motivated strategies for prevention, e.g. locking users out after a certain number of attempts. This work could also reveal interesting tradeoffs between the usability or accuracy of passthoughts and their security.

Finally, our work leaves room for some clear UX improvements. Future work should try using dry electrodes, commonly found in consumer EEG devices, for comfort and usability. The electrodes could be grounded to the ear, instead of the forehead. Additionally, future work could easily place a speaker inside our current custom-fit earbuds to produce working "hearables" that can be used as ordinary headphones.

Future work should also attempt a closed-loop (or online) passthought system, in which users receive immediate feedback on the result of their authentication attempt. A 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 through authentication attempts.

9 Conclusion

As demonstrated by these preliminary results, custom-fit, in-ear EEG earpieces provide three factors of authentication in a single authentication single: thinking one's password, using the discreet form factor of an earpiece. In this paper, we demonstrate quite high authentication accuracy using a single sensing earpiece. By expanding our corpus of EEG readings (in population size, time, and diversity of settings), we hope to better understand the underlying distribution of EEG signals, so that we may better understand the security properties of passthoughts.

References

[1] Akkermans, A. H. M., Kevenaar, T. A. M., and Schobben, D. W. E. Acoustic ear recognition for person identification. In *Proceedings - Fourth IEEE Workshop on Automatic*

Identification Advanced Technologies, AUTO ID 2005 (2005), vol. 2005, pp. 219–223.

[2] ASHBY, C., BHATIA, A., TENORE, F., AND VOGELSTEIN, J. Low-cost electroencephalogram (EEG) based authentication. In *2011 5th International IEEE/EMBS Conference on Neural Engineering, NER 2011* (2011), pp. 442–445.

[3] BOJINOV, H. S. U., SANCHEZ, D. N. U., REBER, P. N. U., BONEH, D. S. U., AND LINCOLN, P. S. Neuroscience Meets Cryptography : Designing Crypto Primitives Secure Against Rubber Hose Attacks. *Proceedings of the 21st USENIX conference on Security symposium* (2012), 1–13.

[4] CHEN, T., AND GUESTRIN, C. XGBoost : Reliable Large-scale Tree Boosting System. *arXiv* (2016), 1–6.

[5] CHUANG, J. One-Step Two-Factor Authentication with Wearable Bio-Sensors, 2014.

[6] CHUANG, J., NGUYEN, H., WANG, C., AND JOHNSON, B. I think, therefore I am: Usability and security of authentication using brainwaves. In *International Conference on Financial Cryptography and Data Security*. 2013, pp. 1–16.

[7] CURRAN, M. T., YANG, J.-K., MERRILL, N., AND CHUANG, J. Passthoughts authentication with low cost eareeg. In *Engineering in Medicine and Biology Society (EMBC), 2016 IEEE 38th Annual International Conference of the* (2016), IEEE, pp. 1979–1982.

[8] FREY, J. Comparison of an open-hardware electroencephalography amplifier with medical grade device in brain-computer interface applications. *Proceedings of the 3rd International Conference on Physiological Computing Systems*, PhyCS (2016), 105–114.

[9] GARRETT, D., PETERSON, D. A., ANDERSON, C. W., AND THAUT, M. H. Comparison of linear, nonlinear, and feature selection methods for EEG signal classification. *IEEE Transactions on Neural Systems and Rehabilitation Engineering 11*, 2 (2003), 141–144.

[10] JOHNSON, B., MAILLART, T., AND CHUANG, J. My thoughts are not your thoughts. *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct Publication - UbiComp '14 Adjunct* (2014), 1329–1338.

[11] KIDMOSE, P., LOONEY, D., JOCHUMSEN, L., AND MANDIC, D. P. Ear-EEG from generic earpieces: a feasibility study. *Conference proceedings : ... Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Annual Conference 2013* (2013), 543–546.

[12] KIDMOSE, P., LOONEY, D., UNGSTRUP, M., RANK, M. L., AND MANDIC, D. P. A study of evoked potentials from ear-EEG. *IEEE Transactions on Biomedical Engineering 60*, 10 (2013), 2824–2830.

[13] KIDMOSE, P., LOONEY, D., UNGSTRUP, M., RANK, M. L., AND MANDIC, D. P. A study of evoked potentials from ear-eeg. *IEEE Transactions on Biomedical Engineering 60*, 10 (2013), 2824–2830.

[14] LOONEY, D., KIDMOSE, P., PARK, C., UNGSTRUP, M., RANK, M., ROSENKRANZ, K., AND MANDIC, D. The in-the-ear recording concept: User-centered and wearable brain monitoring. *IEEE Pulse 3*, 6 (2012), 32–42.

[15] LOONEY, D., PARK, C., KIDMOSE, P., RANK, M. L., UNGSTRUP, M., ROSENKRANZ, K., AND MANDIC, D. P. An in-the-ear platform for recording electroencephalogram. In *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS* (2011), pp. 6882–6885.

[16] MARCEL, S., AND MILLAN, J. D. R. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence 29*, 4 (2007), 743–748.

[17] MARTINOVIC, I., DAVIES, D., FRANK, M., PERITO, D., ROS, T., AND SONG, D. On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. In *Usenixorg* (Berkeley, CA, USA, 2012), Security'12, USENIX Association, pp. 1–16.

[18] MICHALSKA, M. Openbci: Framework for brain-computer interfaces. *University of Warsaw Faculty of Mathematics, Informatics and Mechanics* (2009).

[19] MIKKELSEN, K. B., KAPPEL, S. L., MANDIC, D. P., AND KIDMOSE, P. EEG recorded from the ear: Characterizing the Ear-EEG Method. *Frontiers in Neuroscience 9*, NOV (2015).

[20] MONROSE, F., AND RUBIN, A. Authentication via keystroke dynamics. *Proc. of the 4th ACM Conf. on Computer and Communications Security* (1997), 48–56.

[21] NYMI. Nymi Band - Always-On Authentication.

[22] PALANIAPPAN, R. Electroencephalogram signals from imagined activities: A novel biometric identifier for a small population. In *International Conference on Intelligent Data Engineering and Automated Learning* (2006), Springer, pp. 604–611.

[23] PALANIAPPAN, R. Two-stage biometric authentication method using thought activity brain waves. *International journal of neural systems 18*, 1 (2008), 59–66.

[24] PEIRCE, J. W. Psychopy-psychophysics software in python. *Journal of neuroscience methods 162*, 1 (2007), 8–13.

[25] POULOS, M., RANGOUSSI, M., ALEXANDRIS, N., AND EVANGELOU, A. Person identification from the EEG using nonlinear signal classification. *Methods of information in medicine 41*, 1 (2002), 64–75.

[26] SPIELBERG, S. Minority Report, 2002.

[27] THORPE, J., VAN OORSCHOT, P. C., AND SOMAYAJI, A. Passthoughts: authenticating with our minds. *Proceedings of the 2005 workshop on New security paradigms* (2005), 45–56.

[28] UNITED SCIENCES, L. Aware Hearables - World's First Custom-Fit Bluetooth Headphones with Brain and Body Sensors.

[29] VOIX, J., MALONEY, M., AND TURCOT, M. C. Settable compound delivery device and system for inflatable in-ear device, Aug. 18 2015. US Patent 9,107,772.