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

Your N. Here
Your 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, using brain-based authentication via a custom-fit, in-ear EEG. Across all participants, we achieve mean 0% false acceptance and 0.12% false rejection rates with data from only one earpiece with three electrodes. In a preliminary test of an "imposter" spoofing attack, we find a 0% false acceptance rate. Our results indicate that in-ear EEG could provide a discreet, convenient, multi-factor authentication. (TO ADD: neural source of signal confirmation, usability summary)

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 single-factor authentication using passwords or other user-chosen secrets, the currently dominant method of authentication in consumer applications, face many challenges. Major industry players such as Google and Facebook have strongly encouraged 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. 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 [4]. 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 [9].

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). 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 system we propose and test here uses the choice of a mental task or "passthought" to perform as knowledge, the uniqueness of an individual's brain activity as measured by EEG as inherence, and the physical token of custom-fit earpieces which could easily contain a hardware key-pair as a possession factor. 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.

We find that we can achieve good classification accuracy with a single earpiece containing only three electrodes. More result details.....

2 Related work

We investigate 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 dual knowledge and inherence factors in in previous work, this work includes a 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 by implementing a hardware key-pair. Furthermore, because the earpieces are custom-fitted to each individual, we predicted they would likely not be able to produce good electrical impedances when worn by a different individual.

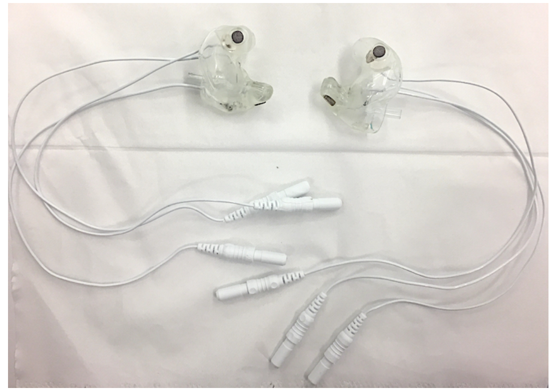

Figure 1: Pair of custom-fit earpieces with 3 embedded electrodes each located at the helix and front-facing and back-facing within the ear canal.

2.1 Passthought authentication

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 [19]. Since 2002, a number of independent groups have achieved 99- 100% authentication accuracy using multi-channel sensors placed on the scalp [18, 14, 17, 2]. In 2013, one group showed that 99% authentication accuracy can also be achieved using a consumer-grade single-channel sensor [5]. 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 multichannel 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) [4].

2.2 In-Ear EEG

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 [13]. 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 [12, 11, 10]. United Sciences is currently developing a consumer ”hearable” (in-ear wearable) called The Aware, which will measure EEG from the ear, among other biometrics [20].

[6] was the first to merge in-ear EEG with passthought authentication, using a single modified consumer grade EEG device among participants and achieving approximately 80 percent authentication accuracy.

2.3 Multi-Factor Authentication in a Single Step

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 [15]. 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) [16]. 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.

3 Methods

3.1 Manufacturing and materials

Custom ear impressions were made by cleaning and injecting silicon into the ear canal. 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.

Is there specifics on how the exactly positions of the electrodes on these pieces were chosen? If not, can simply mention 2 in the ear c

3.2 Study Overview

7 male participants, 5 students and 2 non-students, completed our study protocol approved by the UC Berkeley Committee for Protection of Human Subjects (CPHS). 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 to do a fit and electrical impedance check once earpieces were manufactured, and a third to collect data using the earpieces while participants performed a set of 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.

3.3 Tasks

We used a set of mental tasks based on findings in related work regarding the relative strengths of different mental 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 auditory 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 [**?**], an open-source biosensing system to maintain an overall low cost our set up. OpenBCI has a price tag of about $600, 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 [7]. 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 (a common approach to not bias one side of the head over the other), and using the left mastoid as reference, though we later re-referenced to the right mastoid channel so that our analysis reflects data from a single earpiece. Each earpiece (shown in the image below) contains three channels: one placed on the helix, and two inside the canal - one on the anterior canal wall (front-facing) and the other on the posterior wall (back-facing). The remaining two channels, AGCL ring electrodes, were placed on the right mastoid for later re-referencing, and at approximately Fp1 (the forehead above the left eye) for validating the data collected in the ears against a scalp-based placement. Before beginning the experiment, the data from each channel was visually inspected using the OpenBCI GUI 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. 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

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	Sport-related motor imagery	No	Yes	Closed	Motor
Song	Imagining hearing a song	No	Yes	Closed	Aural
Song - Open	Song task, with eyes open	No	Yes	Open	Aural
Speech	Imagining a spoken phrase	No	Yes	Closed	Aural
Listen - Noise	Listening to noise modulated at 40 Hz	Yes	No	Closed	None
Face	Imagine a person's face	No	Yes	Closed	Visual
Sequence	Imagine face, a 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.

the sport, song, face, speech, and sequence tasks and reminded the participant of these for the second set of trials.

After the completion of the experiment, a subset of participants completed a usability questionnaire asking about the 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 ear EEG and this method of authentication, level of comfort wearing the earpieces, and any other comments they chose to provide.

	Impedances [kOhm]					
	Left ear			Right ear		
Subject	Helix	Front	Back	Helix	Front	Back
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.

4 Analysis

4.1 Validating the data TODO (Update beyond pilot participants

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 using two tests: good impedances measured for the ear electrodes, and alpha-band 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 very good.

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 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. 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 of one participant for example.

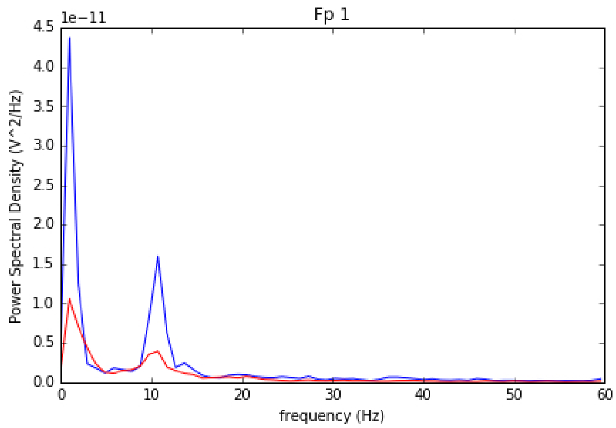

Figure 2: Alpha-attenuation (8-12 Hz range) in Fp1 channel, referenced at left mastoid, for comparison to ear channels. Red indicates breathing data with eyes open, blue indicates the same task with eyes closed.

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 are linear [8], we used XGBoost, a tool for logistic linear classification [3].

To produce feature vectors, we took slices of 100 raw values from each electrode (about 500ms of data), and performed an FFT to produce power spectra for each electrode during that slice. We concatenated all electrode power spectra together, and performed PCA on all concatenated vectors such that the resulting vectors described 95% of the variance in the full power specrum 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 preprocessing.

We trained the classifier using a balanced sample of positive and negative examples, where positive examples were from the target subject and target task, and negative examples were randomly selected tasks from any subject besides the target subject. 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 classification error. After cross-validation, the updated classifier (with paramters applied) predicted labels on each sample in the test set, and we calculated FAR and FRR on its results.

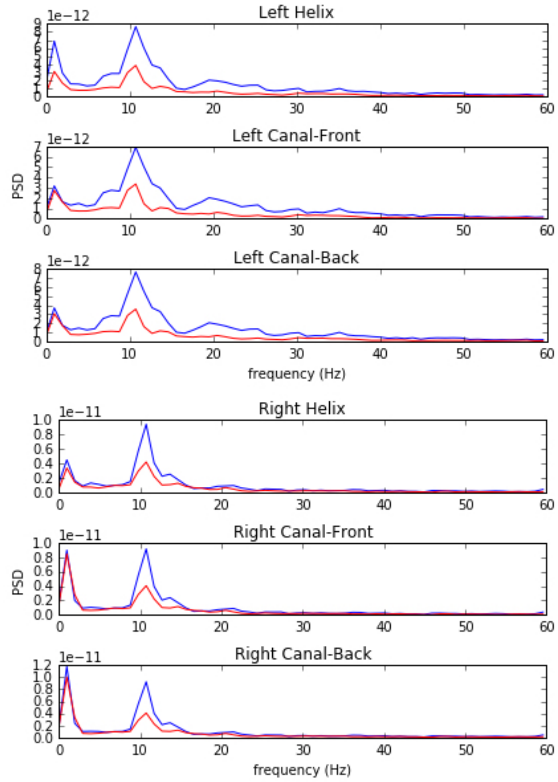

Figure 3: Alpha-attenuation (8-12 Hz range) in left and right ear canal channels, referenced at opposite mastoids respectfully. Red indicates breathing data with eyes open, blue indicates the same task with eyes closed.

5 Results

5.1 Combinations of electrodes

For each configuration of electrodes, we calculated the mean FAR and FRR across all subjects using each task as the passthought (Figure 4). 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. Interestingly, 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.

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 as an earbud. As such, we focus on results from the left ear alone in our following analysis.

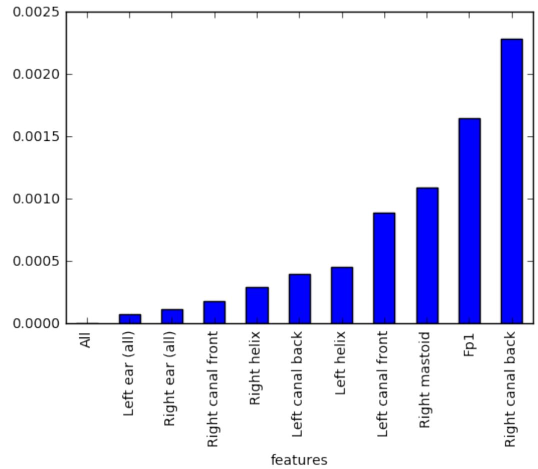

Figure 4: FAR by electrode configuration. All electrodes combined achieves a perfect score. We achieve the next best scores using data from the left ear only.

5.2 Authentication results in the left-ear

In the previous section, we trained and tested a passthought classifier with each task as the passthought, for all subjects. 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).

FAR	FRR	subject	task
0.0	0.0	1	Listen - noise
0.0	0.0	2	Breathe
0.0	0.0	3	Breathe
0.0	0.0	4	Breathe
0.0	0.012	5	Breathe
0.0	0.0	6	Breathe
0.0	0.0	7	Breathe

Table 3: Best-case passthought FAR and FRR results by participant using data from the left ear.

Breathe appeared as the best task across all participants. 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 subjects. All best-performing tasks in our set achieved perfect FAR and FRRs, with the exception of subject 5, whose best-performing task (breathe) had a nonzero FRR.

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

	Original	Within-tasks	Within-subjects
FAR	0.000074	0.000724	0.00252
FRR	0.00442	0.001522	0.0397

Table 4: Mean FAR and FRR for all subjects and pssthoughts across three different training strategies.

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

6 Imposter attack

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

To explore this scenario, we chose one subject (subject 6), and referred to their report of chosen passsthoughts. One subject, drawn from the initial subject pool, performed each of subject 6's passthoughts (simulating an "inside imposter"). Following the same classification and preprocessing steps, we generated 200 samples per task for our imposter, using data from all left ear electrodes.

Since every subject 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 subject 6's classifiers (Table 5). We find no successful spoof attempts for tasks with a chosen secret (e.g., song, face). However, we also do not find any successful spoof attacks for tasks with no chosen secret (e.g., breathe). 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 subject 6's classifiers.

However, since this subject'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

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

Table 5: False acceptance rate for spoofed versions of Subject 6's passthoughts, performed by an inside imposter (from the original subject pool) and an outsid eimposter (not from the original subject pool).

the same protocol with a subject who did not appear in our initial set of subjects (an "outside imposter," Table 5). Again, we do not find any successful authentication attempts.

7 TODO Usability

Quantitative and qualitative data, where appropriate

8 Discussion

Our findings demonstrate the apparent feasibility of single earpiece, achieving good results with only three electrodes and a reference, all on the left ear. FARs and FRRs are low across all subjects and tasks, with FARs overall lower than FRRs. Subjects' best-performing passthoughts typically seeing no errors in our training. Furthermore, no spoofed attacks were successful in our cursory analysis.

The powerful interactions between inherence and knowledge emerged in our spoofing attack. Although our target subject 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 friend the original subject had chosen. For the song tasks, though the song was known, the spoofers did not know what part of the song the original subject 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 ofr spoofing passthoughts.

In our analysis, some notable patterns emerged. First, *breathe* tended to be the best-performing task among participants. Classifiers overall distinguished the breath task even compared to breath tasks from other subjects, implying that the task is expressed differently for each subject, i.e. that this task has an inherence factor sufficient for authentication, even though the task does not have a knowledge factor. 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, the use of conductive gel results in low impedances on other subjects' custom-fit earpieces, despite the uniquness of ear canal shapes between individuals [1]. Nevertheless, classifiers appear to resists spoofing attacks, indicating that task-related signals are unique to individuals. In the future, the custom-fit earbuds could include a hardware keypair to sign authentication attempts, providing a more secure method for establishing the posession factor in our three-factor, one-step scheme.

Finally, performance on Fp1 was not as high as performance in the ear, despite Fp1's popularity in past work on passthoughts [5]. 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.

9 Future Work

One primary question surrounds how our passthought system performance will change with a greater number of users, and with more diverse data. Our system specifically trains on negative examples of non-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. 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 general 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 and accuracy of certain passthoughts with their security properties.

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. 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 during multiple authentication attempts.

10 TODO Conclusion

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

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

[5] 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.

[6] CURRAN, M. T., YANG, J.-K., MERRILL, N., AND CHUANG, J. Passthoughts Authentication with Low Cost EarEEG. *EMBC 2017*.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

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

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

[18] 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.

[19] 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.

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