One-Step, Three-Factor Authentication in a Single Earpiece

Max T. Curran
BioSENSE Lab
School of Information
University of California, Berkeley
Berkeley, CA 94720, USA
mtcurran@ischool.berkeley.edu

Swapan Gandhi
Starkey Hearing Resaerch Center
Berkeley, CA 94724, USA
Swapan_Gandhi@starkey.com

Nick Merrill
BioSENSE Lab
School of Information
University of California, Berkeley
Berkeley, CA 94720, USA
ffff@berkeley.edu

John Chuang
BioSENSE Lab
School of Information
University of California, Berkeley
Berkeley, CA 94720, USA
chuang@ischool.berkeley.edu

Abstract

Multifactor authentication presents a robust method to secure our digital private information, but typically requires multiple actions on the part of the user resulting in a high cost to usability and limiting adoption. Furthermore, a truly usable system must be unobtrusive and inconspicuous. Here, we present a system that provides all three factors of authentication (knowledge, possession, and inherence) in a single step in the form of an earpiece which implements brain-based authentication via custom-fit, in-ear electroencephalography (EEG). We demonstrate its potential by collecting electroencephalography (EEG) data using manufactured custom-fit earpieces with embedded electrodes. Across 7 participants, we are able to achieve perfect performance, mean 0% false acceptance (FAR) and 0% false rejection rates (FRR), using participants' best performing tasks with data from only one earpiece with three electrodes. Our results indicate that a single earpiece with embedded electrodes could provide a discreet, convenient, and robust method for secure one-step, three-factor authentication.

Author Keywords

multifactor authentication; passthoughts, usable security

ACM Classification Keywords
H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous

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 authenticators in two separate steps has frustrated wide adoption due to its additional hassle to users. In this study we undertake, to the best of our knowledge, the first ever exploration 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 "passthought", we seek to achieve all three factors of authentication in a single step by the user. Furthermore, the form factor of an earpiece carries significantly less stigma versus scalp-based passthoughts systems. Technology worn in the ear is already an acceptable practice, for example earphones or bluetooth headsets.

Related Work
The use of EEG as a biometric signal for user authentication has a relatively short history. In 2005, Thorpe et al. motivated and outlined the design of a passthoughts system [16]. Since 2002, a number of independent groups have achieved 99-100% authentication accuracy for small populations using research-grade and consumer-grade scalp-based EEG systems [15, 9, 1, 3].

The concept of in-ear EEG was introduced in 2011 with a demonstration of the feasibility of recording brainwave signals from within the ear canal [8]. The in-ear placement can produce signal-to-noise ratios comparable to those from conventional EEG electrode placements, is robust to common sources of artifacts, and can be used in a brain-computer interface (BCI) system based on auditory and visual evoked potentials [7]. An 80% accuracy level was achieved for user authentication using in-ear EEG captured with a modified single-channel consumer-grade device [4].

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 [12]. 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) [13]. However, as far as we know, no one has proposed or demonstrated a one-step three-factor authentication scheme.

Methods
To create the custom-fitted earpieces, a molding of each participant's ear was taken, 3D scanned, and the earpieces were manufactured with three AgCl electrodes installed in each, two in the ear canal and one at the concha, at positions simplified from those described in [11]. One of the

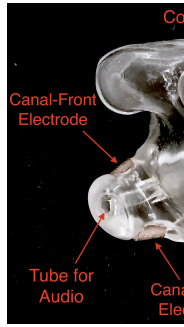

Figure 1: Labeled p
our manufactured cu
earpieces with 3 em
electrodes located i
front-facing (anterio
canal, and back-faci
in the ear canal.

manufactured earpieces is shown in Figure 1.

We used an 8-channel OpenBCI system [10], an open-source alternative to medical-grade EEG systems with demonstrated effectiveness [5]. The ground was placed at the center of the forehead, approximately AFz according to the 10-20 International Standard for Electrode Placement (ISEP), and reference on the left mastoid. One AgCl ring electrode was placed at approximately Fp1 (ISEP location above the left eye) to validate the data collected in the ear against a common scalp-based placement. Before beginning the experiment, the data from each channel was visually inspected using the OpenBCI interface. Audio stimuli were delivered through small tubes in the earpieces. Stimuli were presented using PsychoPy [14]. Participants performed a set of mental tasks we chose based on findings in related work regarding the relative strengths of different tasks in authentication accuracy and usability as reported by participants. [3, 4] 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. Our strategy was to select tasks that captured a diversity across dimensions of external stimuli, involving a personal secret, eyes open or closed (due to known effects on EEG), and different types of mental imagery. All tasks were performed for five trials each, followed by another set of five trials each to reduce boredom and repetition effects. Each trial was 10 seconds in length, for a total of 10 trials or 100 seconds of data collected per task. Seven male participants (P1-P7) completed this study protocol approved by our local ethics review board.

Analysis

We validated data collected by the earpieces using the alpha-attentuation method. It is a well-known feature of EEG data that activity in the alpha-band (approx. 8-12 Hz) increases when the eyes are closed compared to when the eyes are open. We compared data from the *breathe* task with that of the *breathe - open* task. This attenuation is clearly visible even in just a single trial's data from our earpieces and matches data seen in our Fp1 scalp electrode as shown in figure 2.

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 brain-computer interfaces (BCI) are linear [6], we used XGBoost, a popular tool for logistic linear classification [2]. 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. 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 and the updated classifier predicted labels on each sample in the test set. We calculated FAR and FRR from its results.

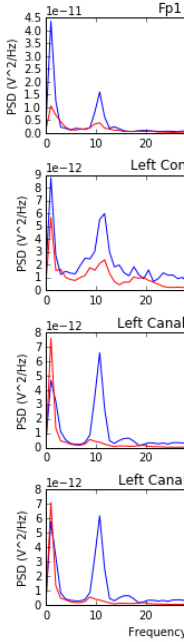

Figure 2: Alpha-atte
(8-12 Hz range) in le
Fp1 channels, refere
mastoid. Red indica
data with eyes open
indicates the same t
closed.

	P1		P2		P3		P5		P7	
Task	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR
Breathe	0.0002	0	0	0	0	0	0	0.0127	0	0
Breathe - open	0.0002	0.0127	0	0	0	0	0	0.0253	0	0
Face	0.0002	0.0253	0.0005	0.0253	0	0.0127	0	0	0	0
Listen	0	0	0.0005	0	0	0	0	0	0	0
Sequence	0	0.0506	0.0002	0	0	0	0	0	0.0007	0.0127
Song	0.0002	0.0380	0	0	0	0	0	0.0127	0.0007	0.0127
Song - open	0.0002	0.0127	0	0	0	0	0	0	0	0.0127
Speech	0.0002	0	0.0005	0	0	0	0	0	0	0
Sport	0.0002	0	0	0	0	0	0	0	0	0.0127
Best Task	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Table 1: FAR and FRR performance of each task for each participant using data from the left ear. P4 and P6 achieve perfect zero FARs and FRRs across all tasks and so are not shown here.

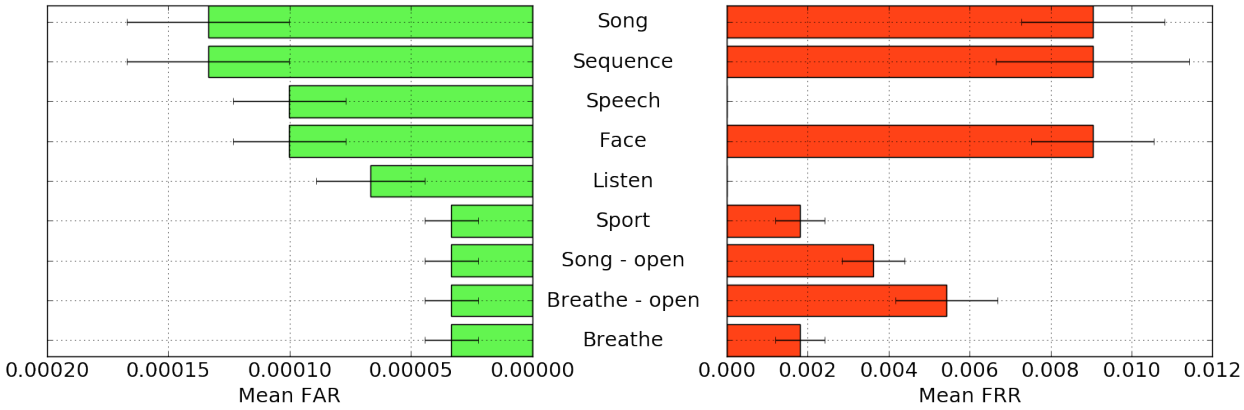

Figure 3: FAR and FRR results by task, across all subjects, using data from the left ear only.

Results

The performance of each task for each participant is shown in Table 1. For each participant we find at least one task for which they achieve 0% FAR and FRR. We also calculated the mean FAR and FRR across all participants for each task, shown in Figure 3.

Discussion & Limitations

Our findings demonstrate the apparent feasibility of a passthoughts system consisting of a single earpiece with 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. Several tasks performed exceedingly well among participants, even tasks like *listen* and *breathe* which didn't have an explicit secondary knowledge factor like in *sport* or *song*. This suggests a passthoughts system could present users with an array of options for them to choose from, though it remains to be seen how these tasks scale with larger populations.

The real-world implications of this study are limited by the small, relatively homogeneous sample of participants. In the case of this initial evaluation however, the homogeneity of our participant pool strengthens the reported results given that system is meant to distinguish between individuals. In order to establish the validity of this system for widespread real-world use we feel it is necessary to expand the size and diversity of participants in future work.

Future Work

Our work leaves room for some clear user experience improvements. Future work should assess dry electrodes, commonly found in consumer EEG devices, for comfort and usability. The electrodes could be grounded to the earlobe, instead of the forehead. Speakers could also be placed inside our current custom-fit earbuds to produce working "hearables" that could 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 would assist in understanding how human learning effects side might impact authentication performance, as the human and machine co-adapt.

Conclusion

As demonstrated by these preliminary results, custom-fit, in-ear EEG earpieces can provide three factors of security in one highly usable step: thinking one's passthought, using the discreet form factor of an earpiece. Among this initial sample, we are able to achieve 100% authentication accuracy using a single sensing earpiece, showing potential for integration with technology already used in everyday life (like earphones). 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 and security properties of passthoughts as well usability issues that may arise in different contexts.

Acknowledgments

The authors would like to thank the Center for Long-Term Cybersecurity for funding this research.

REFERENCES

1. Corey Ashby, Amit Bhatia, Francesco Tenore, and Jacob Vogelstein. 2011. Low-cost electroencephalogram (EEG) based authentication. In *IEEE/EMBS Conference on Neural Engineering*. 442–445.

2. Tianqi Chen and Carlos Guestrin. 2016. XGBoost : Reliable Large-scale Tree Boosting System. *arXiv* (2016), 1–6.

3. John Chuang, Hamilton Nguyen, Charles Wang, and Benjamin Johnson. 2013. I think, therefore I am: Usability and security of authentication using brainwaves. In *International Conference on Financial Cryptography and Data Security*. 1–16.

4. Max T. Curran, Jong-kai Yang, Nick Merrill, and John Chuang. 2016. Passthoughts authentication with low cost EarEEG. In *Proc. of the IEEE Engineering in Medicine and Biology Society Conf.* 1979–1982.

5. Jérémy Frey. 2016. Comparison of an open-hardware electroencephalography amplifier with medical grade device in brain-computer interface applications. PhyCS (2016), 105–114.

6. Deon Garrett, David A. Peterson, Charles W. Anderson, and Michael H. Thaut. 2003. 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.

7. Preben Kidmose, David Looney, Michael Ungstrup, Mike Lind Rank, and Danilo P. Mandic. 2013. A study of evoked potentials from ear-EEG. *IEEE Transactions on Biomedical Engineering* 60, 10 (2013), 2824–2830.

8. D. Looney, C. Park, P. Kidmose, M. L. Rank, M. Ungstrup, K. Rosenkranz, and D. P. Mandic. 2011. An in-the-ear platform for recording electroencephalogram. In *Proc. of the IEEE Engineering in Medicine and Biology Society Conf.* 6882–6885.

9. Sébatien Marcel and José del R Millan. 2007. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29, 4 (2007), 743–748.

10. Magdalena Michalska. 2009. OpenBCI: Framework for Brain-Computer Interfaces. *University of Warsaw Faculty of Mathematics, Informatics and Mechanics* (2009).

11. Kaare B. Mikkelsen, Simon L. Kappel, Danilo P. Mandic, and Preben Kidmose. 2015. EEG recorded from the ear: Characterizing the Ear-EEG Method. *Frontiers in Neuroscience* (2015).

12. F. Monrose and A. Rubin. 1997. Authentication via keystroke dynamics. *Proc. of the 4th ACM Conf. on Computer and Communications Security* (1997), 48–56.

13. Nymi. 2016. Nymi Band - Always-On Authentication. (2016). `https://nymi.com`

14. Jonathan W Peirce. 2007. PsychoPy-psychophysics software in Python. *Journal of neuroscience methods* 162, 1 (2007), 8–13.

15. M Poulos, M Rangoussi, N Alexandris, and a Evangelou. 2002. Person identification from the EEG using nonlinear signal classification. *Methods of information in medicine* 41, 1 (2002), 64–75.

16. Julie Thorpe, P C Van Oorschot, and Anil Somayaji. 2005. Pass-thoughts: authenticating with our minds. *Proc. of the New Security Paradigms Workshop* (2005), 45–56.