2017 UbiComp/ISWC'17 Adjunct September 11–15,
2017Maui, HI, USA10.1145/3123024.3123087
978-1-4503-5190-4/17/09

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

Max T. Curran
Nick Merrill
John Chuang
BioSENSE Lab
School of Information
University of California, Berkeley
Berkeley, CA 94720, USA
mtcurran@ischool.berkeley.edu
ffff@berkeley.edu
chuang@ischool.berkeley.edu

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

Abstract

Multifactor authentication presents a robust security method, but typically requires multiple steps 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 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 collected in one session by 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

usable security; multifactor authentication; passthoughts

ACM Classification Keywords

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

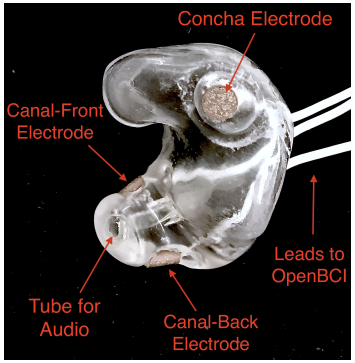

Figure 1: Labeled photo of one of our manufactured custom-fit earpieces with 3 embedded electrodes located in the concha, front-facing (anterior) in the ear canal, and back-facing (posterior) in the ear canal.

Introduction & Related Work

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 chosen secrets, faces many challenges. Major industry players such as Google and Facebook have strongly encouraged their users to adopt two-factor authentication. However, the hassle of submitting authenticators in two separate steps has limited wide adoption.

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), possession factors (e.g., physical tokens, ATM cards), and inherence factors (e.g., biometrics like fingerprints). 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 acceptable, i.e. earphones.

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 [11, 8, 1, 3]. The "passthoughts" term and larger system was proposed in 2005 [12]. The concept of in-ear EEG was introduced in 2011 with a demonstration of the feasibility of recording EEG from within the ear canal [7]. 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 [6]. In 2016, 80% authentication accuracy was achieved using in-ear EEG captured with a modified single-channel device [4]. Behavioral authentication methods such as keystroke dynamics and speaker authentication also fall into the categeory of one-step two-factor, as they include both a knowledge factor (password), and inherence factor (typing rhythm, voice) [10]. To our knowledge, the current work is the first to propose a one-step, three-factor system.

Data Collection

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 [9]. One of the manufactured earpieces is shown in Figure 1. For EEG data collection we used the 8-channel OpenBCI system with 3 channels for the ear electrodes, ground placed at the forehead, reference on the left mastoid, and one additional AgCl ring electrode placed above the left eye ("Fp1") to collect scalp-based data to validate against. Participants performed a set of 9 mental tasks we selected using both previous work [3, 4] and with the aim of diversifying across dimensions: an external stimulus, a personal secret, open or closed eyes, and varied mental imagery. Each task was performed 5 times, then again 5 times each to reduce boredom and repetition effects. Each trial was 10 seconds in length, for a total of 100 seconds of data collected per task. 7 male participants (P1-P7) completed this study protocol approved by the UC Berkeley Committee for Protection of Human Subjects.

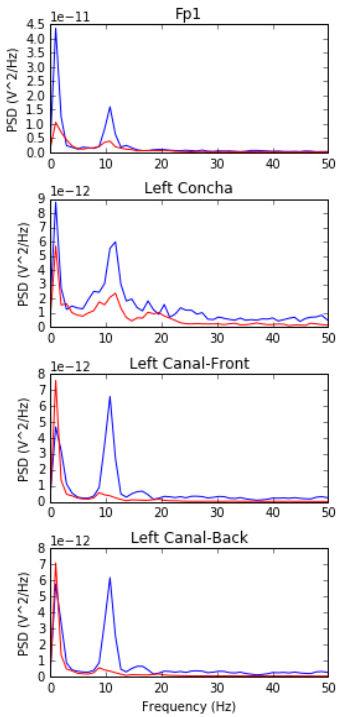

Figure 2: Alpha-attenuation (8-12 Hz range) in left ear and Fp1 channels, referenced at left mastoid. Red indicates breathing data with eyes open, blue indicates the same task with eyes closed.

Analysis

We validated our ear EEG data by comparing the *breathe* task (relaxed breathing, eyes closed) with that of the *breathe - open* task (relaxed breathing, eyes open). Alpha-attenuation, an established metric in EEG work, 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. For the authentication analysis we used XGBoost, a popular tool for logistic linear classification [2], since past work in BCI have shown task classification to be linear [5]. Our feature vectors were power spectra of 100 raw values from each electrode (500 ms of data) which were concatenated together before principal component analysis. With 200 samples per participant, per task, we trained the classifier using a balanced sample of positive (target participant target task) and negative (random task from any participant) examples. We witheld one third of data for testing, and the remaining training set we fed into XGBoost's cross-validation method to predict labels on each test sample.

Results

For each participant we found at least 1 task for which they achieved both 0% FAR and FRR, and two participants, P4 and P6, had perfect performance across all tasks. Generally, FRRs were higher than FARs, though even the highest FRR was only 6%, and the highest FAR less than 1%. By task, *breathe*, *breathe - open*, *song - open* (imagining a chosen song, eyes open), and *sport* (imagining performing a chosen activity) on average achieved the lowest FAR results, while the lowest mean FRRs were *speech* (imagining a chosen phrase) and *listen* (listening to white noise). For all tasks, both mean FAR and FRR were less than 1%. These results appear to establish knowledge and inherence factors, as the correct participant using the wrong task failed to authenticate. Additionally, we found evidence of a possession factor by testing P1's classifier with P1 performing his own passthoughts but using P6's earpiece, and P6's classifier with P1 performing P6's passthoughts using P6's earpiece. In both cases, we found zero successful attempts.

Discussion & Future Work

Our findings demonstrate the feasibility of a passthoughts system consisting of a single earpiece in the ear. FARs and FRRs were 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 see no errors in our test. 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, though this system is meant to distinguish between individuals it is encouraging how well it performs. For real-world authentication, training and testing data should be drawn from different time points days, weeks, and months apart. Future work should also investigate dry electrodes, commonly found in consumer EEG devices, for comfort and usability, or try earpieces that also work as headphones. An investigation of an online passthoughts system, in which users receive immediate feedback on the result of their attempts would elucidate how human adjustments 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, with potential for integration with technology already used in everyday life, like earphones. By expanding in dimensions of time, population size, 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

This work was funded by the Hewlett Foundation through the UC Berkeley Center for Long-Term Cybersecurity.

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. 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.
6. 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.
7. 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.
8. 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.
9. 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).
10. F. Monrose and A. Rubin. 1997. Authentication via keystroke dynamics. *Proc. of the 4th ACM Conf. on Computer and Communications Security* (1997), 48–56.
11. 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.
12. 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.