For educational or research purposes only
Saulynas, S. & Kuber, R. Towards BCI and Gestural-Based Authentication for Individuals who are Blind.
In Proceedings of the 19th International ACM Conference on Computers and Accessibility – ASSETS'17,
Baltimore, MD, 403-404.

Towards Brain-Computer Interface (BCI) and Gestural-Based Authentication for Individuals who are Blind

Sidas Saulynas and Ravi Kuber
UMBC
Baltimore MD 21250
{saulyn1, rkuber} @umbc.edu

ABSTRACT
This paper describes an exploratory study examining the feasibility of using Brain-Computer Interface (BCI) and gestural technologies to support individuals who are blind during the authentication process. Four legally-blind participants were asked to don the Emotiv Epoc headset, and authenticate entry using gestural cues, emotional cues and mental commands. Findings highlighted that while BCI and gestural technologies may be slower and less accurate to use compared to four digit PINs, levels of perceived security were higher, as some of these cues were thought to be more difficult for third parties to replicate. A trade-off between perceived security and usability was evident.

CCS Concepts
CCS → Human-centered computing → Accessibility → Empirical studies in accessibility.

Keywords
Authentication; Blind; Brain-Computer Interface technologies; Gestural technologies;

1. INTRODUCTION
Maintaining privacy and control of one's data has become more of a challenge due to the number of threats present. Tokens which are inputted for device authentication are vulnerable to various eavesdropping or observation attacks [6]. Protecting one's data from being compromised requires users to be vigilant of their surroundings. However, for individuals who are blind, difficulties are faced during this process. In addition to the threat of observation attacks which may go undetected, any negative interaction experience when accessing authentication mechanisms can be exacerbated for blind users due to such factors as restrictions imposed by assistive technologies and inappropriate design of authentication interfaces [4].

If tokens could be entered inconspicuously, input would be less vulnerable to observation attacks. Brain-Computer Interface (BCI) technologies offer potential to support the authentication process. Thoughts cannot be viewed by observers. No other current input modality possesses this true inconspicuous input quality [5], which offers promise to users whose visual channel is blocked or restricted. In this paper, we describe a study examining the feasibility of BCI and gestural technologies, as an alternative input modality for inputting a 4-token authentication code.

ASSETS '17, October 29-November 1, 2017, Baltimore, MD, USA

ACM ISBN 978-1-4503-4926-0/17/10.
https://doi.org/10.1145/3132525.3134785

2. RELATED WORK
Through a series of semi-structured interviews, Ahmed et al. [1] revealed that when considering physical privacy, blind users' concerns include lack of independence (reliance on others) and worries regarding eavesdropping from others. To provide more accessible alternatives for authentication, technologies have been developed to support individuals with visual impairments. Examples include the PassChords solution [2] where authentication tokens are entered by tapping several times on a touch surface with one or more fingers. Other solutions include sequences of pin-based patterns, which were shown to be memorable over a period of time [4]. While studies have considered the potential of BCI to support authentication (e.g. Thorpe et al. [7]), these have yet to exploit the range of cues which can be obtained using off-the-shelf technologies or consider the needs of users with diverse abilities. Our study described in this paper, has aimed to examine the feasibility of using the Emotiv Epoc headset [3] for this purpose.

3. METHODOLOGY
Four legally-blind participants were recruited for purposes of the study (3 males, 1 female, mean age: 32.25). They were introduced to the Emotiv Epoc headset and accompanying software. Mental commands, emotional states and facial expressions (termed "gestural cues") can be obtained from the user using the headset.

Table 1. Input tokens used for each authentication task

Type	Token 1	Token 2	Token 3	Token 4
4-digit PIN	2	4	8	9
Facial Exp.	Blink	Smile	Clinch Teeth	Left Wink
Emotion State	Excite	Excite	Frustr.	Engage
Mental Cmd.	Push	Pull	Lift	Drop
Mixed Methods	Lift	Engage	Blink	Push

Participants were then asked to use an adapted version of an authentication interface described in an earlier study [5], where additional auditory cues were presented to provide greater awareness of content on the graphical interface. To simulate as closely as possible, the familiar task of 4-digit authentication, participants were asked to input four prescribed sets of mental commands, emotional states and gestural cues (termed "tokens"). These needed to be entered in a prescribed order to authenticate entry (see Table 1). The process would terminate after all four tokens were detected or would automatically time out if any token took longer than two minutes to detect. Each cue type was tested separately as well as one authentication task that was a mixture of all three. As a control, 4 digit PINs were also entered by participants. Prior to the authentication tasks, approximately 20-

25 minutes was spent practicing the input tokens to be used. Also, there were six training sessions for each mental command token as these needed to be specifically trained and the signature EEG patterns for each participant stored in a profile log [5]. The speed and accuracy of input were recorded. After completion of the task, participants were presented with a 5-point Likert-scale (5=highest) questionnaire relating to levels of perceived security when accessing the solution and the quality of the user experience. Interviews were also performed to solicit suggestions on strengthening the interface.

4. RESULTS & DISCUSSION

The rate of accuracy and task time taken are shown in Table 2. Findings suggest that in comparison to entering a four digit PIN, lower levels of accuracy were experienced and more time was spent when authenticating using BCI and gestural conditions. Entering a sequence of emotional states was found to be faster and entered more accurately compared with the other BCI and gestural conditions. In terms of subjective user experience (Table 3), emotional states and facial expressions were selected as representing the most superior experience, while mental commands were almost unanimously thought to offer a poorer user experience. Detection rates for facial expressions (62.5%) did not vary considerably from emotional states (68.75%). However, they on average took 21 seconds longer to enter, which could be frustrating for users. In terms of perceived security, participants rated the 4-digit PIN condition lowest (1.75 out 5).

Table 2. Performance by condition

Type	Rate of Accuracy	Avg Speed (sec.)	Avg Perceived Security (Likert Scale 1-5 5=*highest*)
4-digit PIN	100.00%	1.455	1.75
Facial Exp.	62.50%	31.01	2.75
Emotion State	68.75%	10.05	4.25
Mental Cmd.	12.50%	54.03	4.50
Mixed Methods	50.00%	26.39	5.00

Table 3: Quality of subjective user experience

Type	Highest Quality Subjective Experience	Lowest Quality Subjective Experience
Facial Exp.	2	1
Emotion States	2	0
Mental Cmd.	0	3
Mixed Methods	0	0

Although the rate of accuracy entering PIN-based authentication stimuli was 100%, worries about third parties viewing or eavesdropping were evident. As one participant noted, "[4-digit PINs are not secure]…because if there is anyone else around…unless you've taken steps…it's not going to be very secure." The mixed condition was found to offer greater levels of perceived security, as there were multiple choices of token which could be selected for an authentication sequence, some which were not visible to third parties (e.g. mental commands, emotional states). One participant commented, "…whatever mental image you've created…even if you have the same mental images as somebody else, the way it's going to be done is not going to be duplicated, as no-one can see it". Responses highlighted that participants were willing to trade-off usability (in terms of task time) for conditions which offer higher levels of perceived security. However, it was thought that BCI and gestural technologies would need to be enhanced considerably, prior to their deployment for purposes of mainstream authentication.

5. CONCLUSION AND FUTURE WORK

This paper described an exploratory study examining the use of a commercially available BCI and gestural headset as a potential means of supporting authentication by individuals who are blind. While the findings suggest BCI and gestural technologies may offer promise, the scale of the study was small. The next logical step in the research would be to widen the sample of participants, and to evaluate over a period of time to assess the memorability of self-selected vs researcher-selected tokens.

6. ACKNOWLEDGEMENTS

This work was partly supported through the Office of Naval Research (N00014-15-1-2776). We thank Charles Lechner (UMBC) for his assistance with the development of the system.

7. REFERENCES

[1] Ahmed T., Hoyle R., Connelly K., Crandall D., and Kapadia A. 2015. Privacy concerns and behaviors of people with visual impairments. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 3523-3532, DOI=http://dx.doi.org/10.1145/2702123.2702334.

[2] Azenkot S., Rector K., Ladner R., and Wobbrock J. 2012. PassChords: Secure multi-touch authentication for blind people. In *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility*, 159-166, DOI=http://dx.doi.org/10.1145/2384916.2384945.

[3] Emotiv Epoc. Available: http://www.emotiv.com/

[4] Kuber R. and Sharma S. 2012. Developing an extension to an existing tactile authentication mechanism to support non-visual interaction. In *Proceedings of the IASTED Conference on Human-Computer Interaction*, 190-198, DOI=http://dx.doi.org/10.2316/P.2012.772-009.

[5] Saulynas S. and Kuber R. 2017. Towards the use of brain-computer interface technologies as a potential alternative to pin authentication. *International Journal of Human-Computer Interaction*, DOI=http://dx.doi.org/10.1080/10447318.2017.1357905.

[6] Saxena N. and Watt J. H. 2009. Authentication technologies for the blind or visually impaired. In *Proceedings of the USENIX Workshop on Hot Topics in Security*.

[7] Thorpe J., van Oorschot P. C., and Somayaji A. 2005. Pass-thoughts: authenticating with our minds. In *Proceedings of the 2005 Workshop on New Security Paradigms*, 45-56. DOI=http://dx.doi.org/10.1145/1146269.1146282.