Project Description – User Study

Title: Usability and Security of Brainwave-Based Authentication in Real-World Applications
Responsible Investigators: Markus Röse (mroese@mail.uni-paderborn.de), supervised by Prof. Dr. Patricia Arias Cabarcos (pac@mail.upb.de).

Research Problem: In recent years, the market for consumer-grade brain-computer interfaces (BCIs) has seen a rapid rise with numerous manufacturers offering them at different price points. This rise has led to the proposal of using brainwaves as a convenient alternative to passwords [1]. Recent studies have shown that consumer-grade BCIs are not only suitable for this but also show potential for broader acceptance among the general population [2, 3]. Despite these findings combined with the general availability of brain-computer interfaces, there is currently no system implementing a brainwave-based authentication mechanism. This lack leads to usability evaluations often being reduced to a hypothetical exercise.

Goal: The goal of this study is to advance from the theoretical knowledge and study practical challenges in deploying a brainwave-based authentication system in real world scenarios in the form of a master thesis. The evaluated challenges will include both security and usability challenges. In our study we will use a novel prototype implementation of an application supporting brainwave-based authentication. Using this application, study participants can interact with brainwave-based authentication in the real world and give new insights. In addition, we aim to evaluate the security performance of our implementation to supply a baseline for future applications.

Methodology: The planned study is divided into two separate phases, namely an experiment phase followed up by a survey phase. In the experiment phase, participants are asked to interact with a password manager which uses brainwave-based authentication as part of a web browser plugin. After performing an enrolment procedure, in which brainwaves are recorded and temporarily stored, users are asked to perform several authentication tasks to evaluate both the usability and security of the mechanism. Both the enrolment and authentication consist of the participants looking at images while their brainwaves are recorded. Using the browser plugin, we enable participants to authenticate themselves at different web services. The credentials for these web services will be provided by us. This process will take 15-20 minutes, depending on the number of web services visited. Following this, the survey phase starts. Here, participants are asked to fill in a brief survey made up of questions aimed at their perception of the usability and general opinions about the presented application. This will take an added 10-15 minutes.

During both the experiment phase and survey phase, participants will be supervised and can ask for help or instructions if needed. All material used in the study will be provided in both English and German. Recruitment for the study is planned using flyers distributed inside and outside of the university. In addition, we plan to recruit through announcements in lectures and university newsletters. Participants are compensated at a rate of 15EUR/hour. In case a participant decides to abandon the study early, they will be compensated partially equal to their efforts.

Data Analysis and Management: When dealing with participants' data, we adhere to best security and privacy practices. Participants are informed about data processing and must supply written consent in the form of a supplied consent form. Brainwave data collected during the study is immediately

removed after its completion, if not explicitly stated otherwise by the participant in the written consent. During the study, all temporal storage of brainwave data is done locally. At no point is data shared with any of the web services visited during the experiment phase. The data collected during the survey part is collected using the GDPR-compliant LimeSurvey instance hosted by Paderborn University[1]. All survey data is stored in an anonymized form without any personal identifiers. Participants are instructed to not enter any personal information, as answers may be made public as part of the thesis and future publications. In addition to data gathered during the study, we store participants' email addresses to organize the study. These addresses are stored separately from all other gathered data. After completion of the study, all addresses are immediately deleted.

Additional Information: The Study is funded through the chair of IT Security of Paderborn University.

References:

[1] Gui, Q., Ruiz-Blondet, M.V., Laszlo, S. and Jin, Z., 2019. A survey on brain biometrics. *ACM Computing Surveys (CSUR)*, *51*(6), pp.1-38.

[2] P. Arias-Cabarcos, T. Habrich, K. Becker, C. Becker, and T. Strufe, "Inexpensive Brainwave Authentication: New Techniques and Insights on User Acceptance," presented at the 30th USENIX Security Symposium (USENIX Security 21), 2021, pp. 55–72.

[3] J. Chuang, H. Nguyen, C. Wang, and B. Johnson, "I Think, Therefore I Am: Usability and Security of Authentication Using Brainwaves," in *Financial Cryptography and Data Security*, vol. 7862, A. A. Adams, M. Brenner, and M. Smith, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 1–16. doi: 10.1007/978-3-642-41320-9_1.

[1] https://umfragen.uni-paderborn.de

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Standard questionnaire for applications for ethical review by the Paderborn University Ethics Committee

The following standard questionnaire is based largely on the *German Psychological Society's professional ethical guidelines* 7.3.1 to 7.3.9 (DGPs, 2016). Some of the wording of the questions has been taken verbatim from these guidelines. Where this is the case, reference is made to the respective DGPs guidelines in brackets after the relevant question header. The German Association for Experimental Economic Research's (GfeW) standard procedure for reviewing the ethical aspects of research projects (*GfeW review procedure*) (https://gfew.de/ethik) has also been drawn on to design this questionnaire. Appropriate reference is also made here to any questions based on the GfeW review procedure.

Please answer all of the 15 questions below by ticking "Yes" or "No".

Applicant: Markus Röse

Short project title: Usability and Security of Brainwave-Based Authentication in Real-World Applications

	Yes	No
1. Preliminary examination (GfeW Question 1): Has the planned study already been examined and rejected by another ethics committee?	☐	☑
2. Voluntary nature (DGPs 7.3.3): Can it be guaranteed that the subjects' participation in the study is voluntary?	☑	☐
3. Consent (DGPs 7.3.3): Will informed (written) consent be obtained from the subjects regarding participation in the study and data collection?[1]	☑	☐
4. Undisclosed participation (DGPs 7.3.3 and 7.3.6): Will subjects participate in the study without being informed of their participation at the time at which the research project is conducted or without having given their explicit consent to participate (e.g. experimental field studies, covert observations)?	☐	☑

1 Explicit consent may be waived "(1) if it is reasonable to assume that participation in the research will not cause any harm or inconvenience beyond everyday experience, and if the research relates to (a) common educational methods, curricula or teaching methods in the education sector; (b) anonymous questions/questionnaires, independent observations or archive material, the disclosure of which does not expose the participants to any risk of criminal or civil liability, financial loss, professional disadvantage or reputational damage and where confidentiality is guaranteed; (c) factors affecting work and organisational efficiency in organisations, the investigation of which cannot cause any professional disadvantage to the participants and where confidentiality is guaranteed, or (2) if the research is otherwise permitted by laws and regulations" (DGPs, 2017, pg. 22). If any of these reasons apply, then a short application may be submitted, even if "No" has been ticked for Question 2. Please state the reason why explicit consent is not necessary.

	Yes	No
5. Persons in need of protection (DGPs 7.3.3): Is the study aimed at the participation of subjects who, by law or on account of their physical or mental condition, are not able to give informed consent to participate in the study (e.g. persons under the age of 18 or people with physical or mental disabilities) or who, because of the study design, are otherwise particularly vulnerable (e.g. pregnant women, addicts)?	☐	☑
6. Animal testing: Are any animals involved in the planned project (as study subjects or in any other way)?	☐	☑
7. Information (DGPs 7.3.3 and 7.3.6): Will the subjects be informed of *(a) the purpose of the study; (b) the expected duration of the study and the respective procedure; (c) their right to refuse or terminate participation; (d) foreseeable consequences of non-participation or early termination of participation; (e) foreseeable factors that can reasonably be expected to influence willingness to participate (e.g. potential risk); (f) the expected findings of the study; (g) the guarantee of confidentiality and anonymity and, where applicable, the limits of these; (h) the bonus for participation; (i) the different test groups in experimental studies and (j) who they can contact if they have any questions about the research project and about their rights as* subjects?	☑	☐
8. Deception (DGPs 7.3.8, GfeW Question 4): Will the subjects be deceived about the study content, purpose, method or setting or about the promised participation incentives (e.g. payments for experiments), or will specific information about the study be withheld from them? *(Lack of disclosure of the research hypothesis or hypotheses does not fall into this category.)*	☐	☑
9. Intimacy or risk of stigmatisation (DGPs 7.3.3): Does the study address topics that could be perceived by the subjects as intimate (e.g. stressful personal experiences, sexuality, non-conformity) or stigmatising (e.g. illegal or deviant behaviour)?	☐	☑
10. Psychological stress (DGPs 7.3.3): Is there a risk that the subjects will experience psychological stress, fear, exhaustion or any other negative effects (e.g. triggering of traumatic experiences) beyond everyday levels as a result of participating in the study?	☐	☑
11. Physical risks (DGPs 7.3.3): Will the subjects be exposed to any physical risks (e.g. pain, negative side effects) or any potentially stressful or even harmful procedures (e.g. blood sampling) as a result of participating in the study?	☐	☑
12. Administration of substances (DGPs 7.3.3): Will the subjects be administered any medication, placebos or any other substances as part of the study?	☐	☑
13. Remuneration/participation incentives (DGPs 7.3.7): Will the subjects be offered any financial or other incentives that risk encouraging them to participate through coercion?[2]	☐	☑

2 Incentives are to be regarded as coercive if they are designed in such a way that "it must be assumed that the subject is willing to take risks that they would most likely not have taken without this compensation" (Spickhoff & Knebe, 2014, pg. 158). As a rule, this does not include any incentives that represent reasonable compensation for the subject's travel costs, loss of earnings or time.

	Yes	No
14. Disadvantages in case of non-participation (DGPs 7.3.5): Will non-participation in the study result in any direct disadvantages or negative consequences for the subjects? (*Please note:* If participation is required by the relevant examination regulations, potential participants must be made aware of equivalent alternatives for participating in the study.	☐	☑
15. Option to terminate participation (DGPs 7.3.3): Will the subjects have the option to terminate participation during the course of the study at their own request and without any negative consequences, and is this communicated to them in advance?	☑	☐

If you have *no ticks in the coloured boxes* for any of the questions above, you can submit this document in conjunction with a brief description of the study (0.5 to 1 page; both as a PDF, please) by e-mail to ethik-kommission@upb.de, i.e. standard procedure.

If, on the other hand, you have *ticked the coloured box* for *at least one* of the above questions, you will need to follow the in-depth procedure. In the in-depth procedure, in addition to an informative description of the study (1 to 3 pages), all study documents (data collection instruments, instructions etc.) must be provided. If you are following this procedure, please in particular explain why the aspects of your study for which you have ticked the coloured box in the standard questionnaire above are necessary and how you intend to deal with these from an ethical perspective.

Please tick: Standard or in-depth procedure

☑ All questions in the standard questionnaire have been answered with ticks in the white box. (Standard procedure)

☐ The deviation is explained in an attached application in accordance with the Paderborn University Ethics Committee's guidelines for applicants. (In-depth procedure, where at least one tick in a coloured box)

Please tick: Data privacy

☑ The relevant data privacy regulations are complied with.

Paderborn	27/11/20	
Place	Date	Signature

List of references

DGPs (2016). *German Association of Psychologists' and German Psychological Society's professional ethical guidelines and German Association of Psychologists' professional code of conduct* Göttingen: DPGs. Accessed at https://www.dgps.de/index.php?id=85 on 07/08/2017.

Spickhoff, A., & Knehe, H. M. (2014). Freiwilligkeit bei der Teilnahme/unangemessene Anreize (Voluntary participation/inappropriate incentives). In C. Lenk, G. Duttge, & H. Fangerau (Ed.), *Handbuch Ethik und Recht der Forschung am Menschen* (Handbook on ethics and law for research involving human subjects) (pg. 157-158). Berlin: Springer.