"Open Sesame!": User Perception of Physical, Biometric, and Behavioural Authentication Concepts to Open Doors

Lukas Mecke[1,2], **Ken Pfeuffer**[3], **Sarah Prange**[1,2], **Florian Alt**[1,2,3]
[1]University of Applied Sciences Munich, Germany, {firstname.lastname}@hm.edu
[2]LMU Munich, Germany, {firstname.lastname}@ifi.lmu.de
[3]Bundeswehr University Munich, Germany, {firstname.lastname}@unibw.de

ABSTRACT
In usable security (e.g., smartphone authentication), a lot of emphasis is put on low-effort authentication and access concepts. Yet, only very few approaches exist where such concepts are applied beyond digital devices. We investigate and explore seamless authentication systems at doors, where most currently used systems for seamless access rely on the use of tokens. In a Wizard-of-Oz study, we investigate three different authentication schemes, namely (1) key, (2) palm vein scanner and (3) gait-based authentication (compare Fig. 1). Most participants in our study (N=15) preferred the palm vein scanner, while ranking unlocking with a key and gait-based recognition second and third. Our results propose that recovery costs for a failed authentication attempt have an impact on user perception. Furthermore, while the participants appreciated seamless authentication via biometrics, they also valued the control they gain from the possession of a physical token.

CCS Concepts
•**Security and privacy** → **Access control;** *Biometrics;* Authentication;

Author Keywords
Authentication; (Behavioural) Biometrics; Wizard-of-Oz; User Perception

INTRODUCTION
While many research areas of usable security focus on reducing authentication effort (e.g. on mobile devices), only few research to this topic beyond digital devices exists. One common use case for such authentication with non digital artefacts is unlocking doors. This generally follows the steps: 1) search for the key, 2) pick it out from the pocket, and 3) turn it in the keyhole. Performing those steps both takes time and requires the user to always carry the key (i.e., the authentication token) with them. By using biometric authentication, the process to unlock a door could be done seamlessly and - in contrast to most existing approaches - without requiring to either memorise and enter a PIN or carry a physical token (e.g. a key-card, a smartphone or the aforementioned key).

MUM '18, November 25–28, 2018, Cairo, Egypt

ISBN 978-1-4503-6594-9/18/11…$15.00
DOI: https://doi.org/10.1145/3282894.3282923

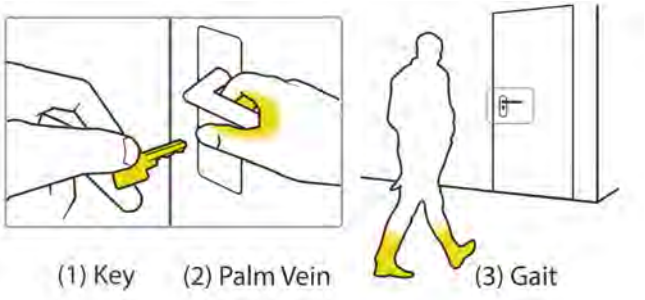

Figure 1. In this work we investigate user perception of different authentication mechanisms at doors. Namely those are (1) a key, (2) a (mock) palm vein scanner and (3) (mock) gait-based recognition. Our results suggest, that users prefer the palm vein scanner while still valuing the possession of a physical token to give them control (key).

Biometric authentication methods make use of users' unique physiological or behavioural traits for identification or authentication purposes [10, 15]. Examples for biometric authentication systems include, but are not limited to, iris scan, facial recognition, fingerprint recognition, touch and gait [2, 4, 9, 13]. While physiological biometrics are increasingly known to the general public since their integration into mobile devices (e.g., fingerprint or face recognition), behaviour based authentication mechanisms are still not widely used but rather seen as an "upcoming field to explore" [2], because of their high false-positives or false-negatives rates. Nonetheless, they are an intriguing option for authentication. Users may not even notice, that they are authenticated at all, leading to a non-intrusive and seamless authentication process [7].

While such transparent authentication systems have been investigated for electronic devices (e.g. [4, 12]), applications for analogue devices are still mostly unexplored. We investigate different mechanisms for unlocking doors as they pose ubiquitous natural access control mechanisms, that require authentication and - as of now - lead to a disruption of user's interaction flow.

In our Wizard-of-Oz study, we assessed the *user perception* of such novel authentication mechanisms for seamlessly unlocking a door. We investigated (1) a physical key as baseline, (2)

a mock palm vein scanner, and (3) mock gait-based authentication. We provide insights towards the user's perception, e.g. with regards to the effect of error recovery effort and the trade-off between using a biometric system and a physical token. Our results propose that users on the one hand like the concept of seamless authentication using biometrics, but on the other hand still appreciate the control they get from possessing a physical key.

RELATED WORK

Biometric Authentication: Palm Vein Scanner

In a survey by Gigya in 2016, 52% of 4000 participants in the US and UK said they would rather not have to remember a PIN or password at all [8]. Instead, they prefer using an alternative form of authentication. Biometric user information such as iris, voice, face, fingerprint or gait can be a quick and secure way to authenticate and avoid the cumbersome and time-consuming task of entering a PIN or using a key [2, 4, 9, 13]. With an estimated 71% of smartphones shipping with biometric authentication in 2018, using biometric authentication has become quite common for many people nowadays [14].

In 1968 the first patent for a palm print identification system was granted to N. Altman [1]. The modern palm vein scanner takes an infrared image of the palm to detect vein patterns that are matched to a saved copy. Romanowski et al. investigated the acceptability and ease-of-use of a palm vein scanner in 2016 [11]. In their study, 75% of the 55 participants found the technology to be non-intrusive, and 77% did not experience any delays during authentication. The company Fujitsu, as a creator of mass-market palm vein scanners, announced in 2018 that they will replace passwords and smartcards for 80,000 employees in their Japanese headquarters in favour of their palm vein scanner PalmSecure [6]. With these efforts showing a high potential, we study palm vein biometric authentication for the purpose of accessing doors.

Behavioural Authentication: Gait-Based Authentication

R.V. Yampolskiy and V. Govindaraju survey the state of behavioral biometrics [17], highlighting gait or stride to authenticate users as a field of research. Initially gait-based recognition became a subject of psychology research in 1977 from J.E. Cutting and L.T. Kozlowski [5], as they noticed that a person could recognise familiar others simply by an abstract display of the movements made while walking. With advances in motion capture technology, gait recognition may be considered as a viable form of behavioural biometrics. Gait motion data can be processed with pattern recognition methods and matched with registered data [3].

A different approach was explored by Weitao Xu et al., who created a gait recognition system for smartwatches, namely "Gait-Watch", that identifies the user's distinct way of moving [16]. This unobtrusive form of gait recognition without the use of visual motion capture shows that integration in general mobile settings can be an option in the future.

A challenge of biometric authentication is the possibility to fake user behaviour to bypass the security mechanism. R.V. Yampolskiy and V. Govindaraju observed that gait-based authentication could be tricked by an impersonator imitating the walk of the registered user [17]. Adding more reference points in the gait-scan and machine learning can increase the accuracy and lower the number of false positives [3]. Natural changes in walking behaviour (e.g. due to mood) can result in false-negatives, severely impairing the user experience [17]. For this reason, biometric authentication often relies on a fallback solution, rendering the security as high as the fallback.

DOOR AUTHENTICATION CONCEPTS

Based on the survey of related work, we identified two novel biometric concepts for authentication that we want to investigate for unlocking doors. As a baseline for doors we use the physical key as it is the most commonly used method nowadays. Both biometric methods are as of now rarely used but have high potential for seamless authentication at doors.

Fingerprint readers require users to actively put their fingers on it. *A palm vein scanner* integrated in a door however would allow seamless authentication by simply pushing and gripping the handle. In comparison, other popular biometric features such as face, voice, or iris ID often require users to either stand still specifically in front of a camera, or do not work in noisy environments. With a palm vein door handle, users benefit from the physical way of gripping the handle that is intuitive to understand because of the handle's physical affordance.

While other proximity based mechanisms (e.g., NFC technologies) require the user to be in small distance of the door, a functional *gait-based system* would authenticate the user by his natural way to approach the door. Behavioural authentication by such motion is often based on probabilistic measure of walking over time, which requires a larger area. However in principle it allows for a completely implicit, i.e. effortless, access through doors.

In both cases, no physical token or remembering and entering a secret would be necessary, which can be a benefit in comparison to the commonly used key.

EVALUATION

The focus of our study is the evaluation of the *user perception* of biometric authentication systems, for which we decided to conduct a Wizard-of-Oz study (i.e., without a working implementation). We tested three different mechanisms to unlock a door, using mock-ups and a physical door barrier controllable by the experimenter.

Study Design

We tested the following independent variables (i.e., unlock mechanisms):

(1) Physical key
(2) Palm vein scanner integrated in the door handle
(3) Gait-based authentication using a Kinect

with the mechanisms (2) and (3) being non functional (i.e. mock-ups). We applied a within-subjects design and counterbalanced the order of authentication mechanisms.

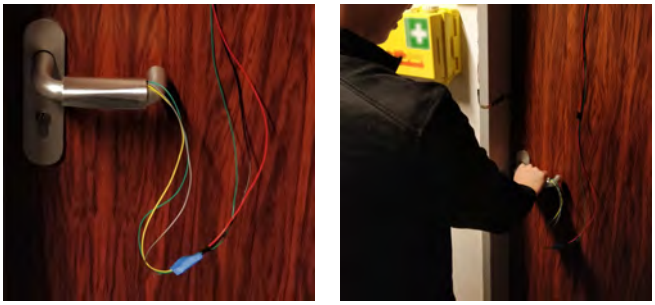

Figure 2. Mock-up of a palm vein scanner, made of a thin sheet of metal with some cushioning. It gripped on the door handle and was connected to the door-lock by visible wires to support the illusion of a running system (left). Participants were asked to grip it to authenticate (right).

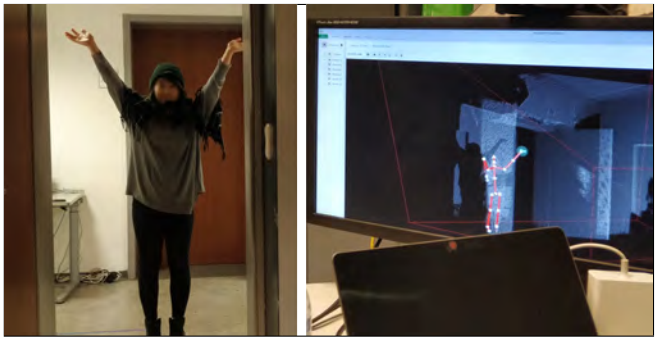

Figure 3. Our setup for the mock gait-based authentication used a Kinect to display the body structure of detected humans in the area to create the impression of a running authentication system.

Rationale

An important aspect of Wizard-of-Oz studies is to offer a system that is as believable as possible in mimicking a real system. To support the impression of a functional system, we added a number of technical enhancements: foil and wires at the door handle mocking the palm vein scanner (Fig. 2), a feedback screen showing the users' skeleton tracked by a Kinect sensor (Fig. 3, LEDs indicating success of authentication) and a mechanical door lock controllable by the experimenter (Fig. 4). Next, we describe the enhancements in detail.

Apparatus

For our study, we used a door with a regular key lock between two rooms. We marked a path and a starting position for the authentication process on the floor with blue tape (see Fig. 5). Participants were asked to walk along this path and unlock the door while walking, using one of the three conditions.

To make participants believe that their actions were unlocking the door we remotely unlocked the door by lifting the mechanical blockade using a wifi connection, as soon as a fully implemented systems would have recognised the user. The micro-controller used for controlling the door lock mechanism was an ESP32 running Arduino software[1]. We offered feedback for condition (2) and (3) in the form of a green LED turning on after successful authentication and a blinking red LED accompanied by a long beep otherwise (Fig. 4, right).

[1] https://www.espressif.com/en/products/hardware/esp32/overview

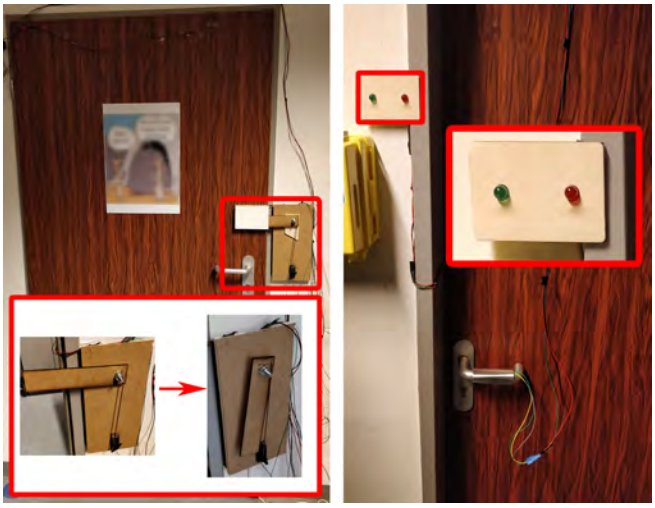

Figure 4. Left: The back view of the door. The mechanical door lock was controlled over a wireless network. Right: The front view of the door. Additional feedback regarding the success of an authentication attempt was provided by coloured lights at the front side. The green LED on the left indicates success, the red LED on the right failure.

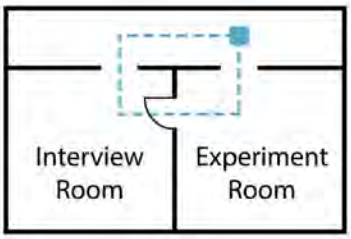

Figure 5. The floor plan we applied in our study setup: Participants were asked to walk along the dotted line from the starting position (rectangle in the top right). Participants had to open the door between experimenters room and interview room using either 1) a key, 2) a (mock) palm vein scanner or 3) (mock) gait-based recognition.

Physical Key: To authenticate, participants had to insert the key into the key hole, rotate it twice, and press the door handle.

Palm Vein Scanner: We mocked the palm vein scanner as a metallic surface embracing the door handle. It was connected to our door-lock by visible wires to support the impression of being functional (compare Fig. 2).

Gait-based Authentication: We placed a Microsoft Kinect[2] in the middle of the experiment room to create the impression of capturing the participants' walking behaviour between the starting position and the locked door. We placed an additional monitor in the experiment room, which displayed the skeleton data captured by the Kinect in real-time (see Fig. 3). The captured data was not used for the authentication but had the sole purpose of giving the users the impression that the system could indeed capture their walking behaviour.

Procedure

As participants arrived at the lab, we firstly introduced the purpose of the study. We then had them fill in a demographic questionnaire. After that, participants were asked to use the

[2] https://developer.microsoft.com/en-us/windows/kinect

	Statement	Rating
1.	The authentication was easy to use.	1...5
2.	The authentication was known.	1...5
3.	The authentication was comfortable to use.	1...5
4.	The authentication was fast.	1...5
5.	The authentication was cumbersome.	1...5
6.	The authentication was secure.	1...5
7.	The authentication was difficult to use.	1...5
8.	I would authenticate using this method.	1...5

Table 1. Questionnaire: We asked participants to rate the above statements. Possible answers were on a 5-point Likert Scale (1: strongly disagree, 2: disagree, 3: neither nor, 4: agree , 5: strongly agree).

different door unlocking mechanisms. The order was counterbalanced. Each mechanism was tested three times. To allow for experiencing situations in which the system failed to authenticate the user, in the conditions palm vein scanner (2) and gait-based authentication (3) we caused one attempt to be unsuccessful with the occurrence again being counterbalanced. Prior to the biometric conditions, participants were required to register themselves by "training the system" (i.e., participants had to use the system for a few times prior to the actual study to make the system "capture their data").

After three successful authentications, we interviewed participants and asked them to fill out a questionnaire. Participants were asked to rate statements from Table 1 (5-Point Likert Scale; 1=strongly disagree; 5=strongly agree). We repeated the questionnaire for all tested unlocking mechanisms.

An additional semi-structured open interview concluded the study session. We asked the participants to compare the three authentication systems and if they saw any dangers or benefits when using biometric techniques to open a door. Afterwards, we asked the participants to explain their ranking of the authentication systems, how each system could be improved, if a combination should be considered, if they would use it in a daily context and if the system(s) felt secure. In the last part of the interview, we asked participants how they would handle different situations. In particular, what would they do in case of a power blackout (for palm vein scan (2) and gait (3)), if they lost their physical key (1), if they suffered from a broken arm (palm vein scan (2)) and if they had additional luggage, which would alter their walking behaviour (3). After the last question, we revealed that it was a Wizard-of-Oz study.

Participants

We recruited 15 participants (Mdn age = 23, 14 Male, 1 Female) for this study; eleven were students with about half of them being enrolled in IT-related degree programs. From our demographics questionnaire we found out that data privacy was an important concern (Mn = 3.47).

RESULTS

Ranking

The results show that participants mostly preferred the palm vein scanner (10 out of 15 participants ranked it as their most preferred authentication method). Four participants preferred the physical key. The least preferred method was gait-based authentication (compare Fig. 6).

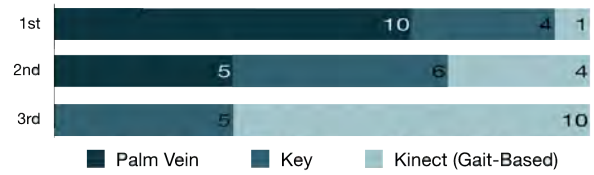

Figure 6. Participants' ranking of the three authentication methods. The palm vein scanner performed best with 10 votes for 1st place.

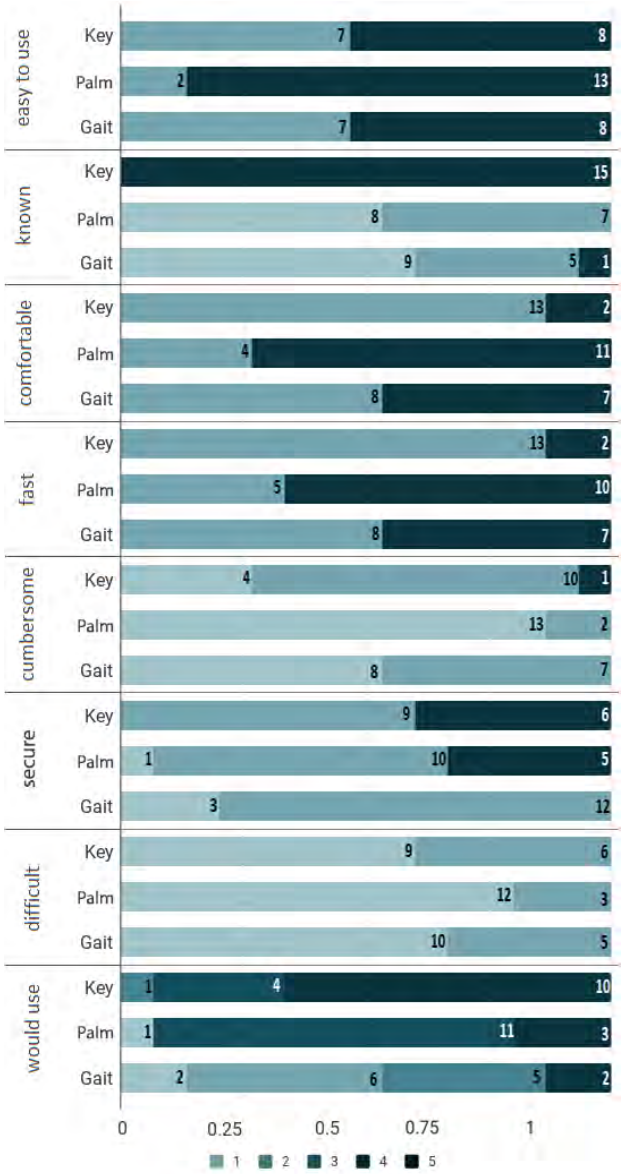

Figure 7. Participants' answers to the statements in Table 1 on a Likert Scale from 1 (strongly disagree) to 5 (strongly agree).

Likert Ratings

The ratings are overall indicative of the ranking (see Tab. 1 for statements and Fig. 7 for results). For the statistical analysis, we used a Friedman test and a Wilcoxon signed-rank test. For the post-hoc multiple comparisons between conditions, we applied Bonferroni corrections (significance level p=.017).

Participants reported all methods to be rather *easy to use* (palm-mn = 4.6, key-mn = 3.6, gait-mn = 3.6), with no statistically significant differences found ($\chi^2(2)$=4.2, p=.12). Similarly, the *difficult to use* question received low ratings (key-mn = 1.4, gait-mn = 1.33, palm-mn = 1.2) with no significant differences ($\chi^2(2)$=2.3, p=.31).

As expected, users had more *knowledge* about the key than the other methods ($\chi^2(2)$=26.8, p=.001). The key was already known by all participants (key-mn = 5), while the other methods were rarely known (gait-mn = 1.6, palm-mn = 1.47). Hence, users had significantly more knowledge about the key than the palm vein scanner (Z=-3.5, p=.001) and the gait-based method (Z=-3.4, p=.002).

Regarding *comfort* ($\chi^2(2)$=26.8, p=.001), users perceived the palm vein scan as most comfortable method (palm-mn = 4.2, gait-mn = 3.6, key-mn = 2.6). This was supported by a statistically significant difference of the key to palm vein scanner (Z=-2.83, p=.005).

For the category *speed* ($\chi^2(2)$=9.8, p=.007), the palm vein scanner was perceived as the fastest method (mn = 4). In comparison, participants perceived the gait-based authentication (mn = 3.4) and the key (mn = 2.4) slower. A statistically significant difference was found between the vein scanner and the key (Z=-2.83, p=.005).

All methods received low scores (key-mn = 1.93, kinect mn= 1.47, palm-mn = 1.13) for being *cumbersome* ($\chi^2(2)$=9.8, p=.007). In addition, the analysis reported a significant difference between the palm vein scanner and the key (Z=-2.67, p=.008), indicating that users found the key slightly more cumbersome.

The results on *security* indicate that users perceive the gait-based method as less secure (mn = 1.8), whereas the other options were rated as moderately secure (palm-mn = 2.93, key-mn = 3.2). The analysis of security ($\chi^2(2)$=8.1, p=.018) revealed that users found the key significantly more secure than gait-based access (Z=-2.4, p=.016).

In real life scenarios ($\chi^2(2)$=17.4, p=.001), users *would use* the key and palm vein scanner (key-mn = 4.6, palm-mn = 4) rather than the gait-based authentication (mn = 2.6). This is supported by the statistical analysis as users rated the the gait method significantly lower than the key (Z=-3.4, p=.001) and the vein scanner (Z=-2.8, p=.004).

User Feedback

Comfort of Use & Reliability

The hand vein scanner was believed to be fast, comfortable and, similarly to the key, moderately secure. The key was also considered moderately fast, but slower than the biometric conditions. Some considered it to be the most cumbersome, feeling burdened by the mechanical task of unlocking the door. The gait-based authentication had mixed opinions in terms of being comfortable, but it was perceived fast, when the authentication worked. However, participants expected the door to open by itself, when they were approaching it (like an automatic sliding door). Participants expressed concerns about the need to always walk in the same fashion to authenticate via their gait. Some felt it was draining to forcefully walk the same way. Others found the method very comfortable to use. Having additional luggage with them did not seem to be a serious concern for the participants. They stated they would put it to the side and authenticate as usual.

Possession & Control

Participants mentioned, that the physical property of a key gave them a feeling of security, as well as enable the option to duplicate and borrow it to others. Using biometric authentication as the sole way of entering a room on the other hand seemed to be intriguing, since they would not have to worry about forgetting or losing a physical key.

Setup Effort

Our biometric authentication mechanisms (i.e., condition (2) and (3)) required a setup process (mocking the process of training a biometric system). The palm vein scanner was familiar to the participants, since most of them compared it to fingerprint scanners used on phones. Hence, the registration process was likewise familiar. Gait-based recognition felt more cumbersome to set up and the participants were worried about false-positives and false-negatives. The registration for biometrics was considered inconvenient by one participant.

Perception of Security

Participants stated the key to be reliable and secure, though a physical token can be lost or forgotten. In contrast, participants appreciated that biometrics cannot be lost but were also worried about exposed data. The gait-based authentication was criticised for being too inconsistent and insecure. Participants were worried about imitators. Some were also concerned about the security of our unlocking mechanisms in general, as locks can be "picked" or technology can be "hacked".

Fallback Solutions

At the end of the interview, we asked, what options participants would consider, if the door could not be unlocked. For the key, every participants had an idea what to do as they could call a lock and key service or use a spare key. In comparison, not everyone could name a backup plan for the biometric techniques. Only some reported they would call a support hotline of the manufacturer of the authentication system. Three participants would allow the manufacturer to remotely open the door if they were locked out. In terms of combinations of the systems, participants suggested that a physical key could be used as a back-up option or that more than two system could be used in sequence to enhance security.

Wizard-of-Oz

When we asked the participants if they had noticed anything strange, two of them stated that they were unsure about the system properly working. However, the participants denied that this had any effect on their answers in the questionnaire. This was the final question we asked before revealing that it was a Wizard-of-Oz study. We observed that the participants were focused on the acoustic and visual feedback and did not try to open the door, when no success signal was given for the biometric mechanisms.

DISCUSSION

We conducted our study as a Wizard-of-Oz setting to assess how users would perceive the usability of three unlocking methods that represent physical, biometric, and behavioural authentication. Our focus is on real world physical door access, that is underexplored in the literature but important considering the amount of doors people access every day. Thus, the main contribution is a better understanding which authentication users prefer, and why. In particular, we summarise our findings on user perception in the following key points:

Main Findings

Users Prefer Biometrics but Keep the Key

The biometric hand vein scanner was the premiere choice for most participants, as it is faster, more comfortable and easier to use compared to the other authentication methods. However, the key was rated higher than the hand vein scanner with regards to which technology participants would actually use. This might be explained by keys offering a moderately secure, fast and comfortable authentication, while also being affordable and known to everyone. Participants knew how to react, if the key was lost and a fallback was needed. In general, the participants valued the possession of a physical object and the option of sharing it. This is not possible for the tested biometric authentication systems.

Recovery Effort Hampers Gait-Based Authentication

Both, the hand vein scanner and the gait-based condition, were criticised for being inconsistent. We assume that the forced failed authentication in our study design led to this observation. Notably, the use of gait was perceived as most inconsistent. If authentication fails, the act of returning to the starting position to walk again compared to the repeated scan of the veins takes a lot more time and effort. It could be helpful to consider alternatives such as a key, when the gait-based authentication fails to work on the first try, as repeating the measurement disrupts a seamless experience. We propose to further investigate the effect of forced fail conditions and error recovery effort as influencing factors on user perception.

Imitation Concerns of Gait

Gait-based authentication was perceived faster and more comfortable to use than the key, but was still ranked last. The reason for this might be the concern of imitators and changes in walking behaviour. Participants were worried, that attackers could mimick their gait to unlock the door, confirming observations of Yampolskiy and Govindaraju [17] . Also, changes in behaviour, such as being injured, could reduce the chance of success dramatically. We propose to further investigate the actual risk from such impersonator attacks as well as adequate fallback options for changes in the user's walking behaviour.

Limitations

Our study comes with some limitations. First, we had a relatively small sample of 15 participants. While this amount resulted in statistically meaningful results on user perception, repeating the study with more participants should provide more reliable data. Further, it is possible that different ages and backgrounds may have an impact on the opinion about authentication systems, demanding further study.

In addition, while we can asses participants' general attitude towards the tested authentication systems, this is but an approximation to how they would react to actual implementations. We carefully crafted our study setup to foster the impression of a real system and increase believability. More studies are needed to cover the range between research prototypes and, in future, novel authentication methods to gain more confidence in how door unlocking mechanisms should be designed.

CONCLUSION

Our Wizard-of-Oz study revealed interesting insights regarding users' perception towards novel, seamless authentication mechanisms for doors. It showed that users are willing to consider biometric mechanisms for seamless authentication at doors. While participants still appreciated the benefits of a physical key, they stated biometric authentication having benefits regarding comfort. In future work, running prototypes of such biometric authentication mechanisms at doors should be evaluated to gain further insights regarding security.

ACKNOWLEDGEMENTS

We thank Oliver Duerr, Andrea Ngao and An Ngo Tien for their help with designing and conducting the study. Work on this project was partially funded by the Bavarian State Ministry of Education, Science and the Arts in the framework of the Centre Digitisation.Bavaria (ZD.B). This research was supported by the Deutsche Forschungsgemeinschaft (DFG), Grant No.: AL 1899/2-1.

REFERENCES

1. Norman G Altman. 1968. Palm print identification system. U.S. Patent US3581282A. (3 December 1968).
2. Parul Arora, Madasu Hanmandlu, and Smriti Srivastava. 2015. Gait based authentication using gait information image features. *Pattern Recognition Letters* 68 (2015), 336–342.
3. Michal Balazia and Petr Sojka. 2018. Gait recognition from motion capture data. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)* 14, 1s (2018), 22.
4. Daniel Buschek, Alexander De Luca, and Florian Alt. 2016. Evaluating the Influence of Targets and Hand Postures on Touch-based Behavioural Biometrics. In *Proc. of CHI '16*.
5. James E Cutting and Lynn T Kozlowski. 1977. Recognizing friends by their walk: Gait perception without familiarity cues. *Bulletin of the psychonomic society* 9, 5 (1977), 353–356.
6. Fujitsu. 2018. Fujitsu Begins Large-Scale Internal Deployment of Palm Vein Authentication to Accelerate Workstyle Transformation. *Fujitsu Press Release* (2018). `http://www.fujitsu.com/global/about/resources/news/press-releases/2018/0118-01.html`.
7. Davrondzhon Gafurov, Einar Snekkenes, and Tor Erik Buvarp. 2006. Robustness of biometric gait authentication against impersonation attack. In *OTM*

Confederated International Conferences "On the Move to Meaningful Internet Systems". Springer, 479–488.

8. Gigya. 2016. Businesses Should Begin Preparing for the Death of the Password. (2016). http://info.gigya.com/rs/672-YBF-078/images/original-201603_gigya_wp_businesses_preparing_death_password-web4.pdf.
9. Anil K Jain, Lin Hong, Sharath Pankanti, and Ruud Bolle. 1997. An identity-authentication system using fingerprints. *Proc. IEEE* 85, 9 (1997), 1365–1388.
10. B Miller. 1988. Everything you need to know about biometric identification. *Personal Identification News 1988 Biometric Industry Directory* (1988).
11. Joseph Romanowski, Kirsanov Charles, Patricia Jasso, Shreyansh Shah, and Hugh W Eng. 2016. A Biometric Security Acceptability and Ease-of-Use Study on a Palm Vein Scanner. *Proceedings of Student-Faculty Research Day, CSIS, Pace University* (2016).
12. Hataichanok Saevanee, Nathan L Clarke, and Steven M Furnell. 2012. Multi-modal behavioural biometric authentication for mobile devices. In *IFIP International Information Security Conference*. Springer, 465–474.
13. S Sanderson and JH Erbetta. 2000. Authentication for secure environments based on iris scanning technology. (2000).
14. Parv Sharma. 2017. Businesses Should Begin Preparing for the Death of the Password. *Counterpoint Press Release* (09 2017). https://www.counterpointresearch.com/.
15. J Wayman. 2000. A definition of biometrics. *National Biometric Test Center Collected Works* 1, 2 (2000), 21–23.
16. Weitao Xu, Yiran Shen, Yongtuo Zhang, Neil Bergmann, and Wen Hu. 2017. Gait-watch: A context-aware authentication system for smart watch based on gait recognition. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*. ACM, 59–70.
17. Roman V Yampolskiy and Venu Govindaraju. 2008. Behavioural biometrics: a survey and classification. *International Journal of Biometrics* 1, 1 (2008), 81–113.