The Feet in Human-Centred Security: Investigating Foot-Based User Authentication for Public Displays

Kieran Watson
2318086w@student.gla.ac.uk
University of Glasgow
Glasgow, United Kingdom

Robin Bretin
r.bretin.1@research.gla.ac.uk
University of Glasgow
Glasgow, United Kingdom

Mohamed Khamis
mohamed.khamis@glasgow.ac.uk
University of Glasgow
Glasgow, United Kingdom

Florian Mathis
florian.mathis@glasgow.ac.uk
University of Glasgow
Glasgow, United Kingdom
University of Edinburgh
Edinburgh, United Kingdom

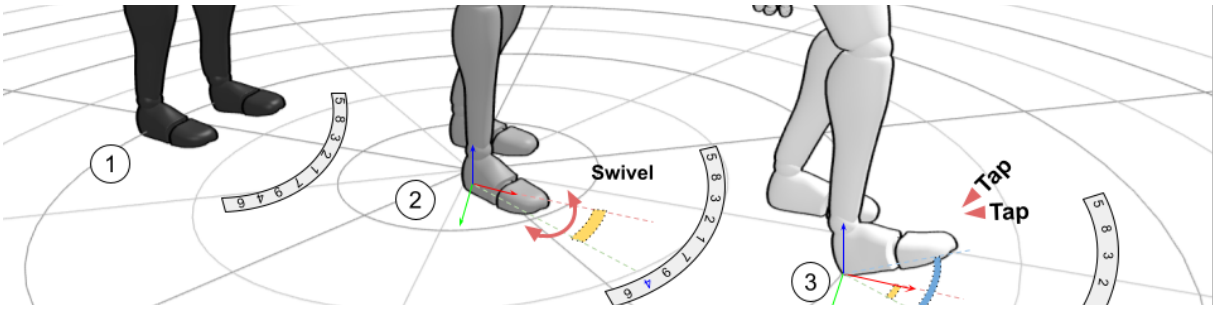

Figure 1: We propose foot-based user authentication for public displays. Users in front of a public display (e.g., ticket machine) (1) provide input using heel rotations (2) and heel taps (3), allowing for unobtrusive and hands-free authentication in public.

ABSTRACT

A large body of work investigated touch, mid-air, and gaze-based user authentication. However, little is known about authentication using other human body parts. In this paper, we investigate the idea of foot-based user authentication for public displays (e.g., ticket machines). We conducted a user study (N=13) on a virtual prototype, *FeetAuth*, on which participants use their dominant foot to rotate through PIN elements (0–9) that are augmented along a circular layout using augmented reality (AR) technology. We investigate *FeetAuth* in combination with three different layouts: *Floor-based*, *Spatial*, and *Egocentric*, finding that *Floor-based FeetAuth* resulted in the highest usability with 4-digit PIN entry as fast as M=6.71 (SD=0.67). Participants perceived foot-based authentication as socially acceptable and highlighted its accessibility. Our investigation of foot-based authentication paves the way for further studies on the use of the human body for user authentication.

CCS CONCEPTS

• **Human-centered computing** → **Human computer interaction (HCI)**; **Virtual reality**; **Empirical studies in interaction design**; • **Security and privacy** → **Usability in security and privacy**.

KEYWORDS

Authentication, Foot-based Interaction, Public Displays

ACM Reference Format:
Kieran Watson, Robin Bretin, Mohamed Khamis, and Florian Mathis. 2022. The Feet in Human-Centred Security: Investigating Foot-Based User Authentication for Public Displays. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3491101.3519838

1 INTRODUCTION

Public displays are a common sight and are growing more widespread in their usage. Many act as vendors for services, accept card payments, and require users to enter a PIN, e.g., when purchasing train tickets on ticket machines or withdrawing cash at automated teller machines (ATMs). The public nature of such displays combined with the lack of usable secure input methods creates a security risk to users' data. Previous research showed that traditional 4-digit

CHI '22 Extended Abstracts, April 29-May 5, 2022, New Orleans, LA, USA

PIN authentications are vulnerable to various threat vectors, including shoulder surfing where a bystander looks over the user's shoulder [8, 12, 30]. Traditional user authentication on public displays (e.g., on a keypad) requires users' hands, which are often already occupied by physical objects (e.g., shopping bags) [10].

In this work, we present the idea of foot-based user authentication and implemented a prototype authentication system called *FeetAuth*. In *FeetAuth*, users use their dominant foot to authenticate by selecting PIN elements (i.e., digits 0 - 9) that are augmented along a circular layout using augmented reality (AR) technology (Figure 1). This means we explore the combination of a private near-eye display (i.e., AR glasses) and foot-based input for usable and secure user authentication in public. The wide-spread adoption of AR glasses in shared and social spaces [21, 43, 64] provides a unique opportunity for the usable security community to utilise AR glasses' affordances for advanced user authentication. For example, AR's private visual channel can be used to convey a unique PIN layout to the user authenticating [65]. To evaluate *FeetAuth*'s initial concept and usability, we exposed participants to a virtual reality (VR) replica of *FeetAuth* and to three different layouts: (1) *Floor-based*, the circular PIN layout is augmented on the floor in front of the public display, (2) *Spatial*, the circular PIN layout is augmented in mid-air 3D space in front of the public display, and (3) *Egocentric*, the circular PIN layout is attached to users' field of view. Our investigation of foot-based user authentication shows that *Floor-based FeetAuth* achieves faster authentications (M=6.71 s, SD=0.67 s) than *Spatial FeetAuth* (M=7.10 s, SD=1.47 s) and *Egocentric FeetAuth* (M=7.72 s, SD=1.14 s). Participants perceived foot-based authentications as a promising alternative to traditional keypad authentication in public and highlighted its accessibility advantages.

Our work provides researchers and practitioners with promising early insights into foot-based user authentication and calls for further research exploring the human body as a whole for usable and secure authentication.

Contribution Statement. **(1)** We propose the idea of foot-based input for user authentication in public and implemented an initial VR prototype, *FeetAuth*. *FeetAuth* is the first system that makes use of users' private near-eye display (i.e., AR glasses) and foot-based interaction for user authentication in public. **(2)** We contribute a VR-powered usability investigation of *FeetAuth* (N=13) and discuss the next steps for (foot-based) user authentication.

2 RELATED WORK

We review previous authentication systems for public displays, works that used VR as a research platform for human-centred research, and prior research on foot-based interaction.

2.1 Secure and Private Interaction in the Public

The usable security community proposed various systems for usable and secure interaction in public. De Luca et al. [11] argued that secure and private interaction on public displays can roughly be divided into three categories: a) software-based solutions (e.g., [9, 31, 51, 58]), b) hardware-based solutions (e.g., [5, 52]), and c) solutions that utilise users' own hardware (e.g., [11, 65]), which are most relevant to our work. Patel et al. [46] proposed a sensor-based authentication mechanism that uses the user's smartphone to authenticate on a public display through a series of shaking gestures. Sharp et al. [55] proposed a system that enables secure and private interaction on a public display by enabling users to view their personal information on their mobile device. De Luca et al. [11] proposed an authentication system that uses users's mobile devices to notify them about false inputs to trick attackers. Although their system increased authentication times due to the added overhead of false inputs (e.g., entering four-digit PIN with 30% lie overhead requires on average 3.91 s (1.70 s) vs. M=2.23 s (0.86 s) for a PIN entry with 0% lie overhead), it increased the resistance against observations. Guerar et al. [20] made use of a QR code that users scan with their mobile device to use colors that correspond to the first and third PIN digit from a color table. A user then matches the second and fourth PIN digits with the color of the first and third digit by rotating a *Color Wheel*. *Color Wheel* maintains a considerable fast authentication speed (M=4.546 s) [20]. *Glass Unlock* by Winkler et al. [65] uses the user's private near-eye display to introduce a secret keypad layout for fast and secure authentication on mobile devices, resulting in authentications as fast as M=2.691 s for a 10-key layout [65]. Khan et al. [32] made use of wearable technology (e.g., Google glasses) for PIN-based authentication on public displays. In their authentication pipeline, a cloud service sends a PIN template to users' wearables. Their system enhanced the security of authentications in public, but the total authentication time was ≈10 s longer than traditional PIN entry [32].

2.2 Virtual Reality as a Research Platform

The HCI community has recently begun conducting user-centred research in virtual environments rather than in physical lab spaces or in the wild. Mäkelä et al. [36] investigated the feasibility of using VR as a research platform to study audience behaviour in front of public displays (i.e., the existence and nature of the honeypot effect [22, 34]). They found that how users notice, approach, and engage with public interactive displays in virtual environments matches to a great extent their behaviour in the real world [36]. Mathis et al. [39] showed that applying a VR-powered usability and security evaluation of a real-world authentication scheme results in similar evaluation findings as an evaluation in the real world (e.g., participants perceived mid-air input as not suitable for user authentication in the public [31, 39]). Rebelo et al. [50] argued that VR enables developing more realistic-looking environments than what is possible in the lab. Fiore et al. [17] showed that virtual environments can overcome the existing challenges around control-mundane realism trade-off and lack of replications in experimental studies. Others argued that VR combines the internal validity of controlled lab studies with the external validity of field studies [17, 36, 40]. There is a plethora of additional works that commented on using VR as a research platform (e.g., [3, 38, 40, 42, 61, 63]).

2.3 Feet in Human-Computer Interaction

Foot-based interaction received significant attention in the broader HCI research field. The two most noted works are Pearson and Weiser's classification of the feet when interacting with mechanical devices [47] and the research landscape paper by Velloso et al. [60]. Foot-based interaction with computer interfaces can be

Figure 2: We evaluated *FeetAuth* in a (virtual) subway station with virtual bystanders to increase authentication realism. (1) shows our simulated *Keypad Authentication*. (2-4) show foot-based user authentication in three different layouts: (2) *Floor-based*, (3) *Spatial*, (4) *Egocentric*. Pointing and selection was performed using heel rotations [25] and toe taps [6].

drawn back to 1967, where English et al. [16] and Engelbart [15] investigated *Knee Control*, an interaction method in which users interact with a workstation using a rocking motion on the ball of the foot. More recent work by Simeone et al. [56] investigated the use of foot movements to support users in their 3D interaction tasks (e.g., object rotation), finding that foot movements are easy to learn, but might introduce a form of the *Midas Touch* problem [33]. Lopes et al. [35] investigated foot-based interaction for contactless hand gesture interaction. Through foot-tapping and heel rotations, participants could perform object manipulations of 3D objects. Feet input can assist hands in clutching tasks, and foot-based gestures come with a precision high enough to perform one-dimensional translations and rotations [35]. Müller et al. investigated foot-taps [44] and lateral shifts of the walking path [45] for hands-free input on head-mounted displays (HMDs). They found that foot-based input provides a viable interaction technique for HMDs. There is a larger body of work that investigated feet input for VR locomotion [62], to zoom and pan maps on public displays [53], to select menu items on mobile devices [54], or for text entry and cursor-positioning in the context of workspaces [48, 49].

3 *FEETAUTH*: CONCEPT & IMPLEMENTATION

We designed and implemented an early prototype of *FeetAuth* to conduct a usability evaluation of foot-based user authentication on public displays. *FeetAuth* combines the strengths of foot-based interaction [60] and AR glasses to support user authentication [65]. Providing users with additional authentication methods that do not require hand input can be particularly valuable as there are many situations in which physical constraints (e.g., shopping bags) already occupy users' hands, not allowing them to apply security measures (e.g., shielding PIN entry) [10].

In *FeetAuth*, users use their foot to select numbers through heel rotations [25] and toe taps [6] (Figure 1). We opted for these gestures as they allow for single foot input, can be performed without much effort, and are suitable even for constrained spaces where physical space is limited. In summary, *FeetAuth* allows for precise pointing and selection of PIN elements through the use of users' dominant foot. Input corrections in *FeetAuth* are performed through heel taps [59]. Below, we discuss *FeetAuth*'s configurations in more detail.

3.1 *FeetAuth*'s Configurations

In all *FeetAuth* configurations PIN elements are augmented along a circular layout in a randomised order (Figure 1). Only the user authenticating has access to the PIN layout, similar to Glass Unlock [65]. We investigate *Floor-based* and indirect (i.e., *Spatial* and *Egocentric*) input on *FeetAuth*, similar to Müller et al. [44].

Keypad Authentication. We use *Keypad Authentication* to imitate real-world PIN entry in a VR environment (baseline). This roughly simulates 4-digit PIN input on a traditional keypad [19]. To provide input, users point with an HTC VIVE controller on one of the keys on the keypad. The virtual laser beam (originating from the centre of the HTC VIVE controller) was used as pointing method, with selection being performed using a trigger press [19].

Floor-based FeetAuth. We augment the PIN elements (0-9) on the floor in front of the public display to allow for a direct mapping between heel rotation and PIN layout (Figure 2-2). Users point on the digits using *heel rotations* [25]. A *toe tap* [6] after a previous digit selection inputs the corresponding digit. A *heel tap* [59] deletes the last input.

Spatial FeetAuth. Here, input works identical to that of *Floor-based FeetAuth* with the difference that the PIN elements are augmented along a circular layout in a fixed position in the 3D space in front of the ticket machine (Figure 2-3). The "physical" digit positions remain the same, but there is no 1:1 mapping between pointing and UI as the circular layout is now positioned in 3D space. Selected PIN elements are highlighted in grey.

Egocentric FeetAuth. Input in *Egocentric* works identical to *Spatial FeetAuth* with the difference that the PIN elements are augmented along a circular layout that is attached to users' head movements. This means users perceive the PIN layout in an egocentric view (Figure 2-4). Selected PIN elements are highlighted in grey.

3.2 Implementation and Apparatus

We implemented a VR prototype of *FeetAuth* in Unity 3D (C#). Previous work by Mäkelä et al. [36] and Mathis et al. [38–40] showed that using VR as a research method to conduct user studies on public displays and to evaluate real-world prototype authentication systems is feasible. A VR-powered research approach also enabled us to conduct research in a relatively realistic environment, which is challenging to replicate in a physical lab. To evaluate foot-based user authentication we created a realistic looking subway setting in which a user authenticates on a public display to purchase a ticket for public transport. We slightly modified a 3D model of a subway station [26] to further increase the realism of such an authentication (e.g., we added a train [24] and additional bystanders using Adobe's MIXAMO library [1]). As hardware we used the HTC VIVE, one HTC VIVE controller when providing input in *Keypad Authentication*, and one HTC VIVE tracker which we attached to users' dominant foot when providing input using *FeetAuth*.

4 METHOD

We recruited N=13 participants through internal mailing lists and social media for a 1-hour study session. To prevent fatigue, we had short breaks (out of VR) after experiencing each *FeetAuth* configuration. Our analysis reported in Section 5 is based on N=12 participants as we had to exclude the participant data of the first user study session due to technical issues. The study was designed as a within-subject experiment with four conditions: 4-digit *Keypad Authentication* (simulated baseline) and the three different layouts to convey the digit arrangements to the user authenticating: *FeetAuth* with a *Floor-based*, *Spatial*, and *Egocentric* layout. Conditions were counter-balanced using a Latin Square [4]. We measured 1) participants' authentication time from the first digit entry to the last, 2) participants' perceived workload when authenticating using the NASA-TLX questionnaire [23], and 3) participants' experience when using *FeetAuth*, i.e., "Input using this method is *easy/natural/pleasant/fast/error prone/usable/comfortable*", answered on a 5-point Likert scale. We concluded with a semi-structured interview guided by the questions in Appendix A. One researcher transcribed the interview data and split participants' statements into meaningful excerpts to then systematically cluster participants' feedback using an affinity diagram. Two additional researchers reviewed and discussed the clustering, which main results we report in 5.4. The study went through an internal Ethics checklist at the University of Glasgow.

4.1 Study Procedure

Participants first filled a questionnaire about their demographics. We then presented the motivation of our study and participants' task using a slide deck. Participants then authenticated ten times for each condition (e.g., ten sequential authentications on *FeetAuth* with *Egocentric*) and went through a training session in advance of each authentication block (similar to [9, 30, 41]). We opted for multiple sequential authentications to increase participants' exposure to the individual configurations while keeping the duration of a user study session as short as possible (e.g., no study session lasted longer than one hour). This is in line with previous works (e.g., [28, 30]). Participants reported their perceived workload [23]) and provided feedback on their experience and the system's usability after each authentication block. The study concluded with a usability ranking of the different configurations (i.e., *FeetAuth* with *Egocentric*) and with a short semi-structured interview (Appendix A).

4.2 Demographics

On average, participants were 26.83 years old (min=19, max=40, SD=6.26). We had four female and eight male participants. Five participants reported to rarely ever use VR, four never used VR before, two use VR once a month, and one participant reported using VR almost every day. We also report our sample's security behaviour using the SEBIS questionnaire [14] and their affinity for technology interaction using the ATI scale [18] to allow for better comparisons and replication studies. The sample's mean security behaviour score was M=3.31 (Md=4.0, SD=1.41) on a scale ranging from 1 to 5 (Device Securement (M=4.31, SD=1.03), Password Generation (M=3.21, SD=1.37), Proactive Awareness (M=2.37, SD=1.26), and Updating (M=3.69, SD=1.09). The technology affinity, ranging from 1 to 6, was M=3.99 (Md=4, SD=1.34).

5 RESULTS

5.1 Authentication Times & Input Corrections

We excluded those authentications that had input corrections to allow for a better comparison between the conditions. There was a significant difference of input times between the different conditions ($F(3,33)=34.966$, $p<0.05$). Post-hoc Bonferroni corrected pairwise comparisons revealed significant differences ($p<0.05$) between *Keypad Authentication* (M=3.99, SD=1.13) and *Floor-based* (M=6.71, SD=0.64), *Keypad Authentication* and *Spatial* (M=7.10, SD=1.41), and *Keypad Authentication* and *Egocentric* (M=7.72, SD=1.09). There was also a significant difference between *Egocentric* and *Floor-based* ($p<0.05$). No other pairs were significant ($p>0.05$). Figure 3 shows the authentication times. Table 1 in Appendix B provides an overview of all authentication times, including those that included input corrections.

We also compared participants' number of corrections when providing input using *FeetAuth*. There is no evidence of a significant difference of the number of digit corrections between the conditions ($F(1.762,19.378)=3.646$, $p= 0.0502$), with M=0.058 (SD=0.086) for *Keypad Authentication*, M=0.417 (SD=0.478) for *Floor-based*, M=0.383 (SD=0.264) for *Spatial*, and M=0.242 (SD=0.232) for *Egocentric*.

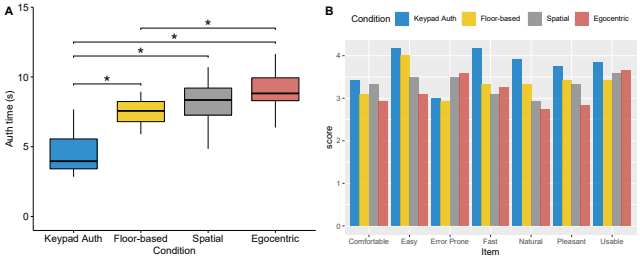

Figure 3: (A) Boxplot of authentication times for correct PIN entries. (B) 5-point Likert scores.

5.2 Perceived Workload

Participants' perceived workload was significantly different between the conditions ($\chi^2(3) = 14.798$, $p<0.05$). Bonferroni corrected pairwise corrections revealed a significant difference between *Keypad Authentication* (M=25.69, SD=23.14) and *FeetAuth* with *Egocentric* (M=48.61, SD=31.64) ($p<0.05$). The values for *Floor-based* and *Spatial* were M=40.35 (SD=30.62) and M=42.22 (SD=28.02), respectively. We proceeded with a comparisons between *Keypad Authentication* and all layouts in *FeetAuth* on the level of each dimension to allow for a more nuanced analysis. A Friedman test revealed a significant effect of condition on participants' mental workload ($\chi^2(3)=16.144$, $p<0.05$), physical workload ($\chi^2(3)=13.844$, $p<0.05$), effort ($\chi^2(3)=12.027$, $p<0.05$), and frustration ($\chi^2(3)=8.258$, $p<0.05$). Bonferroni corrected tests revealed a significant difference of participants' perceived mental workload in *Egocentric* (M=60.833, SD=28.67) and *Floor-based* (M=39.167, SD=27.46), and in *Egocentric* and *Keypad Authentication* (M=28.5, SD=24.41). Physical workload was significantly higher in *Egocentric* (M=58.33, SD=30.25) than in *Keypad Authentication* (M=22.92, SD=22.81). Participants' effort was significantly higher in *Egocentric* (M=58.75, SD=28.69) than in *Keypad Authentication* (M=33.75, SD=25.86). Post-hoc Bonferroni corrected tests did not confirm the differences in participants' frustration ($p>0.05$). Table 1 in Appendix B shows an overview of all raw NASA-TLX values.

5.3 Usability Perception and Ranking

A Friedman test on the 5-point Likert scale responses revealed a significant difference between the conditions in their perceived ease ($\chi^2(3)=9.179$, $p<0.05$) and naturalness ($\chi^2(3)=8.036$, $p<0.05$). However, Bonferroni-corrected pairwise comparisons did not confirm the significant differences ($p>0.05$). Figure 3 shows an overview of participants' responses to the 5-point Likert questions. Participants also ranked the different layouts by perceived usability. A weighted ranking (rank 1 multiplied by $\times 4$, rank 2×3, etc.) resulted in *Keypad Authentication* with the highest score (40), followed by *FeetAuth* with *Floor-based* (36), *FeetAuth* with *Spatial* (28), and *FeetAuth* with *Egocentric* (26). This means that participants preferred the *Floor-based* configuration over the *Spatial* and *Egocentric*, but *Keypad Authentication* was overall preferred.

5.4 Semi-structured Interview

Our affinity diagram resulted in three main themes: *FeetAuth*'s usability, social acceptability, and accessibility. Some participants were concerned about the space required to use *FeetAuth* in public. However, P10, for example, voiced *"I don't think other people would mind it. You're just standing still, you're not getting in anyone's way, the movements are pretty much confined to your own personal space."* (P10). A few participants mentioned that *FeetAuth* can be particularly helpful in situations where touch-less input is preferred. P9 brought up *"hospitals, lots of germs and stuff, especially with COVID less contact would be better."* (P9). Some participants mentioned that traditional keypad authentication might be better for situations where time is important as authentications on *FeetAuth* took longer. Most participants found *FeetAuth* to be socially acceptable in public due to its unobtrusiveness (e.g., only involves subtle heel rotations and taps). P3 voiced that *FeetAuth "would be quite acceptable because it is something most people don't even look at. like if you move around your feet nobody will realise/recognise."* (P3). P10 added they *"did not feel like [they were] doing anything out of the ordinary"* (P10) and P5 mentioned that *"nowadays most people are getting used to using technology more than before and to like use VR and AR."* (P5). However, a few participants were slightly critical about *FeetAuth*'s social acceptability. P7 voiced that *"nowadays [*FeetAuth*] would not be acceptable, people would be looking at you weirdly."* (P7). P11 mentioned it would take some time until people would become used to *FeetAuth*. Overall, participants shared the opinion that *FeetAuth* contributes to accessibility, especially for people who have difficulties using their hands, e.g., *"people who have issues like parkinsons wouldn't be able to properly physically touch the keypad without increased effort."* (P10).

6 DISCUSSION

We applied VR to study *FeetAuth*, an early concept and implementation of foot-based user authentication for public displays. Foot-based authentication takes longer than simulated 4-digit PIN authentication (see 5.1) and introduces a cognitive overhead for user authentication (see 5.2). However, participants were overall positive about using their feet to authenticate in public. The primary aim of this work was to broaden the design space of user authentication by an initial usability and social acceptability study of foot-based input in combination with private near-eye glasses. We consider *FeetAuth* as a complementary authentication method to, e.g., traditional 4-digit PIN authentication, authentication using mid-air gestures [31], two-factor authentication [29, 37], and gaze-based authentication [31], which all have unique advantages and disadvantages (e.g., gaze-based input is highly secure but pervasive eye tracking introduces privacy concerns [27]). Below, we discuss some of the advantages and disadvantages of foot-based user authentication.

6.1 *FeetAuth*'s Usability and Social Acceptability

We noted that participants perceived *FeetAuth* as usable, but that authentications took significantly longer (M=3.99 s for *Keypad Authentication* vs. M=6.71 s for *Floor-based FeetAuth*). *FeetAuth*'s *Floor-based* configuration was faster than *Spatial* and *Egocentric* and it was perceived as a) easier to use, b) less error-prone, c) more natural, and d) slightly more pleasant than *Spatial* and *Egocentric* (Figure 3). Some participants mentioned that *FeetAuth* in combination with a private near-eye display for the PIN layout can be particularly

promising for security sensitive contexts (e.g., government facilities, cash withdrawals at ATMs). Others voiced that *FeetAuth* is a promising alternative to touch-less input at times of COVID. The former, authenticating in security sensitive contexts, can happen infrequently [7, 13]. Therefore, we believe *FeetAuth* can be particularly valuable for privacy-conscious users or in high-risk settings. The vast majority of our participants perceived *FeetAuth* as socially acceptable because of its unobtrusiveness, with some exceptions in crowded places where foot-tapping and heel rotations might require additional physical space. The analysis and the qualitative feedback reported in 5.4 suggest that some specific configurations of *FeetAuth* (e.g. *Floor-based*) do not significantly impact users' perceived workload and input accuracy. The ranking reported in 5.3 suggests that *Floor-based FeetAuth* is to be preferred over *Spatial* and *Egocentric*. Although some of our participants touched on the social acceptability of foot-based input from a bystander's point of view (see 5.4), these comments are solely based on their experience of using the system. Participants did not observe foot-based input as a bystander, which we leave to future work.

6.2 *FeetAuth*'s Accessibility

By extending the design space of user authentication to users' feet we provide users with a complementary authentication method, which can be advantageous in many situations. For example, one participant voiced that *FeetAuth* is particularly promising in situations where elderly people can not use their hands due to disabilities (e.g., the typical Parkinson's tremor which tends to first occur in the hands). Previous work by De Luca et al. [10] highlighted additional contextual factors such as carrying shopping bags that might impact user authentications in public. In such cases, foot-based user authentication offers a promising complementary authentication method despite its shortcoming in authentication speed. As put by Bergman and Johnson, accessibility is defined as *"removing barriers that prevent people with disabilities from participating in substantial life activities, including the use of services, products and information"* [2]. While *FeetAuth* in combination with AR technology might not be universally accessible, leveraging users' whole body for user authentication can contribute to authentication systems that benefit people of all ages and abilities [57].

6.3 Next Steps for (Foot-based) Authentication

Using feet for user authentication, in combination with an augmented private keypad layout, introduces novel privacy concerns and threat vectors that should be addressed before deploying such systems in the wild. Similar to Patel et al.'s [46] and De Luca et al.'s system [11], *FeetAuth* requires a secure communication channel between the user's AR glasses and the public display, which may results in an additional threat vector (e.g., man-in-the-middle attacks). Future work is called to evaluate the feasibility of such an authentication pipeline and consider users' privacy concerns and their willingness of using personal hardware for advanced user authentication. *FeetAuth* makes use of users' private near-eye display to convey a private keypad layout to the user (similar to [65]). However, it remains unclear if users are willing to connect their private hardware to public displays (e.g., ATMs) for improved security. It is also important to acknowledge that a virtual prototype evaluation of *FeetAuth* may not have been able to cover all the rich nuances of a shared social space in the real world. While the use of VR is suitable and valuable for an early concept and evaluation of foot-based user authentication, we encourage future work to consider how reality can be best mimicked in such VR environments. Furthermore, we focused in our work on the usability and social acceptability of foot-based user authentication in public. Follow up research is called to evaluate *FeetAuth*'s security and usability when deployed and embedded into an actual system. One interesting future research direction here is to evaluate *FeetAuth*'s preparation time (i.e., time until first input [65]) when users' authentication is embedded into an actual production task (e.g., withdrawing cash at an ATM [40]).

7 CONCLUSION

We designed, implemented, and evaluated a (VR) prototype, *FeetAuth*, to get insights into the usability and social acceptability of foot-based user authentication in public. A user study showed that *FeetAuth* results in longer authentications than simulated 4-digit PIN authentication on a keypad, but that foot-based authentication in combination with AR technology provides a promising authentication method. We believe our work can inspire usable security researchers and practitioners in designing and implementing novel authentication systems that incorporate the human body, beyond traditional hand input, for user authentication.

ACKNOWLEDGMENTS

We thank all participants for taking part in our research and all reviewers for their valuable feedback. This publication was supported by the University of Edinburgh and the University of Glasgow jointly funded PhD studentships, by the UKRI Centre for Doctoral Training in Socially Intelligent Artificial Agents (EP/S02266X/1), and partially by EPSRC (EP/V008870/1) and PETRAS National Centre of Excellence (EP/S035362/1).

REFERENCES

[1] Adobe. 2022. *Mixamo - Animate 3D characters for games, film, and more.* https://www.mixamo.com accessed 01 January 2022.

[2] Eric Bergman and Earl Johnson. 2001. Towards accessible human-computer interaction. *Sun Microsystems Laboratories The First Ten Years* (2001).

[3] Jim Blascovich, Jack Loomis, Andrew C. Beall, Kimberly R. Swinth, Crystal L. Hoyt, and Jeremy N. Bailenson. 2002. Immersive Virtual Environment Technology as a Methodological Tool for Social Psychology. *Psychological Inquiry* 13, 2 (2002), 103–124. arXiv:https://doi.org/10.1207/S15327965PLI1302_01 https://doi.org/10.1207/S15327965PLI1302{_}_01

[4] James V Bradley. 1958. Complete counterbalancing of immediate sequential effects in a Latin square design. *J. Amer. Statist. Assoc.* 53, 282 (1958), 525–528.

[5] Lynne Coventry, Antonella De Angeli, and Graham Johnson. 2003. Usability and Biometric Verification at the ATM Interface. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Ft. Lauderdale, Florida, USA) *(CHI '03)*. Association for Computing Machinery, New York, NY, USA, 153–160. https://doi.org/10.1145/642611.642639

[6] Andrew Crossan, Stephen Brewster, and Alexander Ng. 2010. Foot tapping for mobile interaction. *Proceedings of HCI 2010 24* (2010), 418–422.

[7] Sauvik Das, David Lu, Taehoon Lee, Joanne Lo, and Jason I. Hong. 2019. The Memory Palace: Exploring Visual-Spatial Paths for Strong, Memorable, Infrequent Authentication. In *Proceedings of the 32nd Annual ACM Symposium on User Interface Software and Technology* (New Orleans, LA, USA) *(UIST '19)*. Association for Computing Machinery, New York, NY, USA, 1109–1121. https://doi.org/10.1145/3332165.3347917

[8] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now You See Me, Now You Don't: Protecting Smartphone Authentication from Shoulder Surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for

Computing Machinery, New York, NY, USA, 2937–2946. https://doi.org/10.1145/2556288.2557097

[9] Alexander De Luca, Katja Hertzschuch, and Heinrich Hussmann. 2010. ColorPIN: Securing PIN Entry through Indirect Input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 1103–1106. https://doi.org/10.1145/1753326.1753490

[10] Alexander De Luca, Marc Langheinrich, and Heinrich Hussmann. 2010. Towards Understanding ATM Security: A Field Study of Real World ATM Use. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (Redmond, Washington, USA) *(SOUPS '10)*. Association for Computing Machinery, New York, NY, USA, Article 16, 10 pages. https://doi.org/10.1145/1837110.1837131

[11] Alexander De Luca, Emanuel von Zezschwitz, and Heinrich Hußmann. 2009. Vibrapass: Secure Authentication Based on Shared Lies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Boston, MA, USA) *(CHI '09)*. Association for Computing Machinery, New York, NY, USA, 913–916. https://doi.org/10.1145/1518701.1518840

[12] Alexander De Luca, Emanuel von Zezschwitz, Ngo Dieu Huong Nguyen, Max-Emanuel Maurer, Elisa Rubegni, Marcello Paolo Scipioni, and Marc Langheinrich. 2013. Back-of-Device Authentication on Smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 2389–2398. https://doi.org/10.1145/2470654.2481330

[13] Gloria Dhandapani, Jamie Ferguson, and Euan Freeman. 2021. *HapticLock: Eyes-Free Authentication for Mobile Devices.* Association for Computing Machinery, New York, NY, USA, 195–202. https://doi.org/10.1145/3462244.3481001

[14] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 2873–2882. https://doi.org/10.1145/2702123.2702249

[15] Douglas Engelbart. 1984. *Doug Engelbart Discusses Mouse Alternatives.* https://invisible-mirror.net/archives/shuford/terminal/engelbart_mouse_alternatives.html accessed 01 January 2022.

[16] W.K. English, D.C. Engelbart, and M.L. Berman. 1967. Display-Selection Techniques for Text Manipulation. *IEEE Transactions on Human Factors in Electronics* HFE-8, 1 (1967), 5–15. https://doi.org/10.1109/THFE.1967.232994

[17] Stephen M. Fiore, Glenn W. Harrison, Charles E. Hughes, and E. Elisabet Rutström. 2009. Virtual experiments and environmental policy. *Journal of Environmental Economics and Management* 57, 1 (2009), 65–86. https://www.sciencedirect.com/science/article/pii/S0095069608000983 Frontiers of Environmental and Resource Economics.

[18] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467.

[19] Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. 2017. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. NDSS.

[20] Meriem Guerar, Mohamed Benmohammed, and Vincent Alimi. 2016. Color wheel pin: Usable and resilient ATM authentication. *Journal of High Speed Networks* 22, 3 (2016), 231–240.

[21] Jan Gugenheimer, Christian Mai, Mark McGill, Julie Williamson, Frank Steinicke, and Ken Perlin. 2019. Challenges Using Head-Mounted Displays in Shared and Social Spaces. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI EA '19)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3290607.3299028

[22] John Hardy, Enrico Rukzio, and Nigel Davies. 2011. Real World Responses to Interactive Gesture Based Public Displays. In *Proceedings of the 10th International Conference on Mobile and Ubiquitous Multimedia* (Beijing, China) *(MUM '11)*. Association for Computing Machinery, New York, NY, USA, 33–39. https://doi.org/10.1145/2107596.2107600

[23] Sandra G Hart and Lowell E Staveland. 1988. Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. In *Advances in psychology*, Vol. 52. Elsevier, 139–183.

[24] HippoStance. 2022. *Subway Bar.* https://sketchfab.com/3d-models/subway-bar-900fcf289b1b4c3cbc7f595684ca033a accessed 04 January 2022.

[25] Scott E. Hudson, Chris Harrison, Beverly L. Harrison, and Anthony LaMarca. 2010. Whack Gestures: Inexact and Inattentive Interaction with Mobile Devices. In *Proceedings of the Fourth International Conference on Tangible, Embedded, and Embodied Interaction* (Cambridge, Massachusetts, USA) *(TEI '10)*. Association for Computing Machinery, New York, NY, USA, 109–112. https://doi.org/10.1145/1709886.1709906

[26] jimbogies. 2022. *Metro / Subway Station.* https://sketchfab.com/3d-models/metro-subway-station-b975322ae1ca417c82641cbc7e172ff6 accessed 04 January 2022.

[27] Christina Katsini, Yasmeen Abdrabou, George E. Raptis, Mohamed Khamis, and Florian Alt. 2020. *The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions.* Association for Computing Machinery, New York, NY, USA, 1–21. https://doi.org/10.1145/3313831.3376840

[28] Mohamed Khamis, Florian Alt, Mariam Hassib, Emanuel von Zezschwitz, Regina Hasholzner, and Andreas Bulling. 2016. GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 2156–2164. https://doi.org/10.1145/2851581.2892314

[29] Mohamed Khamis, Regina Hasholzner, Andreas Bulling, and Florian Alt. 2017. GTmoPass: Two-Factor Authentication on Public Displays Using Gaze-Touch Passwords and Personal Mobile Devices. In *Proceedings of the 6th ACM International Symposium on Pervasive Displays* (Lugano, Switzerland) *(PerDis '17)*. Association for Computing Machinery, New York, NY, USA, Article 8, 9 pages. https://doi.org/10.1145/3078810.3078815

[30] Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. 2017. GazeTouchPIN: Protecting Sensitive Data on Mobile Devices Using Secure Multimodal Authentication. In *Proceedings of the 19th ACM International Conference on Multimodal Interaction* (Glasgow, UK) *(ICMI '17)*. Association for Computing Machinery, New York, NY, USA, 446–450. https://doi.org/10.1145/3136755.3136809

[31] Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zezschwitz, Jens Le, Andreas Bulling, and Florian Alt. 2018. CueAuth: Comparing Touch, Mid-Air Gestures, and Gaze for Cue-Based Authentication on Situated Displays. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4, Article 174 (dec 2018), 22 pages. https://doi.org/10.1145/3287052

[32] Rasib Khan, Ragib Hasan, and Jinfang Xu. 2015. SEPIA: Secure-PIN-authentication-as-a-service for ATM using mobile and wearable devices. In *2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*. IEEE, 41–50.

[33] Rick Kjeldsen and Jacob Hartman. 2001. Design Issues for Vision-Based Computer Interaction Systems. In *Proceedings of the 2001 Workshop on Perceptive User Interfaces* (Orlando, Florida, USA) *(PUI '01)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/971478.971511

[34] Hannu Kukka, Heidi Oja, Vassilis Kostakos, Jorge Gonçalves, and Timo Ojala. 2013. What Makes You Click: Exploring Visual Signals to Entice Interaction on Public Displays. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 1699–1708. https://doi.org/10.1145/2470654.2466225

[35] Daniel Lopes, Filipe Relvas, Soraia Paulo, Yosra Rekik, Laurent Grisoni, and Joaquim Jorge. 2019. FEETICHE: FEET Input for Contactless Hand GEsture Interaction. In *The 17th International Conference on Virtual-Reality Continuum and Its Applications in Industry* (Brisbane, QLD, Australia) *(VRCAI '19)*. Association for Computing Machinery, New York, NY, USA, Article 29, 10 pages. https://doi.org/10.1145/3359997.3365704

[36] Ville Mäkelä, Sheikh Radiah Rahim Rivu, Saleh Alsherif, Mohamed Khamis, Chong Xiao, Lisa Marianne Borchert, Albrecht Schmidt, and Florian Alt. 2020. Virtual Field Studies: Conducting Studies on Public Displays in Virtual Reality. In *Proceedings of the 38th Annual ACM Conference on Human Factors in Computing Systems* (Honolulu, Hawaii, USA) *(CHI '20)*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3313831.3376796

[37] Karola Marky, Martin Schmitz, Verena Zimmermann, Martin Herbers, Kai Kunze, and Max Mühlhäuser. 2020. *3D-Auth: Two-Factor Authentication with Personalized 3D-Printed Items.* Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376189

[38] Florian Mathis, Joseph O'Hagan, Mohamed Khamis, and Kami Vaniea. 2022. Virtual Reality Observations: Using Virtual Reality to Augment Lab-Based Shoulder Surfing Research. In *2022 IEEE Virtual Reality and 3D User Interfaces (VR)*.

[39] Florian Mathis, Kami Vaniea, and Mohamed Khamis. 2021. *RepliCueAuth: Validating the Use of a Lab-Based Virtual Reality Setup for Evaluating Authentication Systems.* Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445478

[40] Florian Mathis, Kami Vaniea, and Mohamed Khamis. 2022. Can I Borrow Your ATM? Using Virtual Reality for (Simulated) In Situ Authentication Research. In *2022 IEEE Virtual Reality and 3D User Interfaces (VR)*.

[41] Florian Mathis, John H. Williamson, Kami Vaniea, and Mohamed Khamis. 2021. Fast and Secure Authentication in Virtual Reality Using Coordinated 3D Manipulation and Pointing. *ACM Trans. Comput.-Hum. Interact.* 28, 1, Article 6 (jan 2021), 44 pages. https://doi.org/10.1145/3428121

[42] Florian Mathis, Xuesong Zhang, Joseph O'Hagan, Daniel Medeiros, Pejman Saeghe, Mark McGill, Stephen Brewster, and Mohamed Khamis. 2021. Remote XR Studies: The Golden Future of HCI Research?. In *Proceedings of the CHI 2021 Workshop on XR Remote Research. http://www. mat. qmul. ac. uk/xr-chi-2021*.

[43] Mark McGill and Stephen Brewster. 2019. Virtual Reality Passenger Experiences. In *Proceedings of the 11th International Conference on Automotive User Interfaces and Interactive Vehicular Applications: Adjunct Proceedings* (Utrecht, Netherlands) *(AutomotiveUI '19)*. Association for Computing Machinery, New York, NY, USA,

434–441. https://doi.org/10.1145/3349263.3351330

[44] Florian Müller, Joshua McManus, Sebastian Günther, Martin Schmitz, Max Mühlhäuser, and Markus Funk. 2019. Mind the Tap: Assessing Foot-Taps for Interacting with Head-Mounted Displays. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300707

[45] Florian Müller, Martin Schmitz, Daniel Schmitt, Sebastian Günther, Markus Funk, and Max Mühlhäuser. 2020. *Walk The Line: Leveraging Lateral Shifts of the Walking Path as an Input Modality for Head-Mounted Displays.* Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3313831.3376852

[46] Shwetak N. Patel, Jeffrey S. Pierce, and Gregory D. Abowd. 2004. A Gesture-Based Authentication Scheme for Untrusted Public Terminals. In *Proceedings of the 17th Annual ACM Symposium on User Interface Software and Technology* (Santa Fe, NM, USA) *(UIST '04)*. Association for Computing Machinery, New York, NY, USA, 157–160. https://doi.org/10.1145/1029632.1029658

[47] G. Pearson and M. Weiser. 1986. Of Moles and Men: The Design of Foot Controls for Workstations. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Boston, Massachusetts, USA) *(CHI '86)*. Association for Computing Machinery, New York, NY, USA, 333–339. https://doi.org/10.1145/22627.22392

[48] G. Pearson and M. Weiser. 1986. Of Moles and Men: The Design of Foot Controls for Workstations. *SIGCHI Bull.* 17, 4 (apr 1986), 333–339. https://doi.org/10.1145/22339.22392

[49] G. Pearson and M. Weiser. 1988. Exploratory Evaluation of a Planar Foot-Operated Cursor-Positioning Device. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Washington, D.C., USA) *(CHI '88)*. Association for Computing Machinery, New York, NY, USA, 13–18. https://doi.org/10.1145/57167.57169

[50] Francisco Rebelo, Paulo Noriega, Emília Duarte, and Marcelo Soares. 2012. Using Virtual Reality to Assess User Experience. *Human Factors* 54, 6 (2012), 964–982.

[51] Volker Roth, Kai Richter, and Rene Freidinger. 2004. A PIN-Entry Method Resilient against Shoulder Surfing. In *Proceedings of the 11th ACM Conference on Computer and Communications Security* (Washington DC, USA) *(CCS '04)*. Association for Computing Machinery, New York, NY, USA, 236–245. https://doi.org/10.1145/1030083.1030116

[52] Hirokazu Sasamoto, Nicolas Christin, and Eiji Hayashi. 2008. Undercover: Authentication Usable in Front of Prying Eyes. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy) *(CHI '08)*. Association for Computing Machinery, New York, NY, USA, 183–192. https://doi.org/10.1145/1357054.1357085

[53] Johannes Schöning, Florian Daiber, Antonio Krüger, and Michael Rohs. 2009. Using Hands and Feet to Navigate and Manipulate Spatial Data. In *CHI '09 Extended Abstracts on Human Factors in Computing Systems* (Boston, MA, USA) *(CHI EA '09)*. Association for Computing Machinery, New York, NY, USA, 4663–4668. https://doi.org/10.1145/1520340.1520717

[54] Jeremy Scott, David Dearman, Koji Yatani, and Khai N. Truong. 2010. Sensing Foot Gestures from the Pocket. In *Proceedings of the 23nd Annual ACM Symposium on User Interface Software and Technology* (New York, New York, USA) *(UIST '10)*. Association for Computing Machinery, New York, NY, USA, 199–208. https://doi.org/10.1145/1866029.1866063

[55] Richard Sharp, James Scott, and Alastair R. Beresford. 2006. Secure Mobile Computing Via Public Terminals. In *Pervasive Computing*, Kenneth P. Fishkin, Bernt Schiele, Paddy Nixon, and Aaron Quigley (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 238–253.

[56] Adalberto L. Simeone, Eduardo Velloso, Jason Alexander, and Hans Gellersen. 2014. Feet movement in desktop 3D interaction. In *2014 IEEE Symposium on 3D User Interfaces (3DUI)*. 71–74. https://doi.org/10.1109/3DUI.2014.6798845

[57] Molly Follette Story. 2001. Principles of universal design. *Universal design handbook* (2001).

[58] Desney S Tan, Pedram Keyani, and Mary Czerwinski. 2005. Spy-resistant keyboard: more secure password entry on public touch screen displays. In *Proceedings of the 17th Australia conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future*. Citeseer, 1–10.

[59] Yanbo Tao, Tin Lun Lam, Huihuan Qian, and Yangsheng Xu. 2012. A real-time intelligent shoe-keyboard for computer input. In *2012 IEEE International Conference on Robotics and Biomimetics (ROBIO)*. IEEE, 1488–1493.

[60] Eduardo Velloso, Dominik Schmidt, Jason Alexander, Hans Gellersen, and Andreas Bulling. 2015. The Feet in Human–Computer Interaction: A Survey of Foot-Based Interaction. *ACM Comput. Surv.* 48, 2, Article 21 (sep 2015), 35 pages. https://doi.org/10.1145/2816455

[61] Alexandra Voit, Sven Mayer, Valentin Schwind, and Niels Henze. 2019. *Online, VR, AR, Lab, and In-Situ: Comparison of Research Methods to Evaluate Smart Artifacts.* Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300737

[62] Julius von Willich, Martin Schmitz, Florian Müller, Daniel Schmitt, and Max Mühlhäuser. 2020. *Podoportation: Foot-Based Locomotion in Virtual Reality.* Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376626

[63] Maximilian Weiß, Katrin Angerbauer, Alexandra Voit, Magdalena Schwarzl, Michael Sedlmair, and Sven Mayer. 2021. Revisited: Comparison of Empirical Methods to Evaluate Visualizations Supporting Crafting and Assembly Purposes. *IEEE Transactions on Visualization and Computer Graphics* 27, 2 (2021), 1204–1213. https://doi.org/10.1109/TVCG.2020.3030400

[64] Julie R. Williamson, Mark McGill, and Khari Outram. 2019. *PlaneVR: Social Acceptability of Virtual Reality for Aeroplane Passengers.* Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3290605.3300310

[65] Christian Winkler, Jan Gugenheimer, Alexander De Luca, Gabriel Haas, Philipp Speidel, David Dobbelstein, and Enrico Rukzio. 2015. Glass Unlock: Enhancing Security of Smartphone Unlocking through Leveraging a Private Near-Eye Display. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1407–1410. https://doi.org/10.1145/2702123.2702316

A SEMI-STRUCTURED INTERVIEW QUESTIONS

Our semi-structured interviews at the end of the study were roughly guided by the following questions. Questions were added or omitted where appropriate.

(1) How socially acceptable would you perceive the use of this system to be in a real world scenario?
(2) Can you think of any scenarios where it would not be socially acceptable?
(3) Can you think of any advantages or disadvantages to using this system over keypad authentication?
(4) Can you name any scenarios where foot based authentication would be preferable over the traditional method (and vice versa)?
(5) Do you have any final thoughts or notes you would like to share?

B MEASURES: OVERVIEW

Table 1: NASA-TLX scores for each dimension, authentication times with no corrections, authentication times with corrections, and the number of corrections applied to all PIN entries. Values represent mean (standard deviation).

Measure	Keypad	Floor	Spatial	Egocentric
NASA-TLX				
Mental Demand	28.75 (SD=24.41)	39.17 (SD=27.46)	47.08 (SD=26.84)	60.83 (SD=28.67)
Physical Demand	22.92 (SD=22.81)	55.00 (SD=33.57)	48.33 (SD=33.12)	58.33 (SD=30.25)
Temporal	28.33 (SD=23.96)	44.17 (SD=31.75)	42.08 (SD=24.44)	42.92 (SD=34.28)
Performance	18.75 (SD=15.24)	28.74 (SD=30.61)	27.92 (SD=25.17)	26.25 (SD=27.73)
Effort	33.75 (SD=25.86)	46.25 (SD=27.23)	51.67 (SD=15.17)	58.75 (SD=28.69)
Frustration	21.67 SD=26.40)	28.75 (SD=30.01)	36.25 (SD=30.09)	44.58 (SD=31.29)
Overall NASA-TLX Score	25.69 (SD=23.14)	40.35 (SD=30.62)	42.22 (SD=28.02)	48.61 (SD=31.64)
Authentications				
Auth. Times (w/o corrections)	3.99 (SD=1.13)	6.71 (SD=0.64)	7.10 (SD=1.41)	7.72 (SD=1.09)
Auth. Times (with corrections)	13.14 (SD=7.41)	15.04 (SD=3.15)	17.15 (SD=8.32)	17.11 (SD=2.43)
Number of Corrections	0.06 (SD=0.09)	0.42 (SD=0.48)	0.38 (SD=0.26)	0.24 (SD=0.23)