"If It Wasn't Secure, They Would Not Use It in the Movies" – Security Perceptions and User Acceptance of Authentication Technologies

Verena Zimmermann(✉) and Nina Gerber

Faculty of Human Sciences, Technische Universität Darmstadt, Darmstadt, Germany
{zimmermann, n.gerber}@psychologie.tu-darmstadt.de

Abstract. Whereas the text password is still ubiquitous as authentication scheme, its shortcomings are well-acknowledged within the research community. A plurality of alternatives such as other knowledge-based, token-based or biometric authentication schemes have been developed. Although the usability of these schemes has been analyzed, the results concerning further user perceptions are complex and somewhat ambiguous. Further, most of these results stem from focus groups and surveys where the actual interaction with the systems was not tested. To shine light on this topic we conducted a laboratory study with 35 participants to compare and understand user perceptions of several biometric and non-biometric authentication schemes. We simulated the interaction with authentication schemes to protect our participants' data and to avoid affecting influences of particular implementations. The results showed that the text password is still popular among the participants for reasons of familiarity and due to privacy aspects, namely because no personal information has to be provided. Fingerprint and iris recognition were well liked among the biometrics by many participants due to the perceived security of using a unique feature for authentication. However, the use of personal information also raised privacy concerns in others. This leads to the assumption that there might be two user groups preferring either passwords or biometrics. The assumption along with possible influencing variables such as authentication context or familiarity should be addressed in future research. The simulation of authentication schemes could further be improved by addressing realistic error rates to increase external validity of the study design.

Keywords: Authentication · Biometrics · Security · Perception · Acceptance

1 Introduction

Even though passwords as a classical form of authentication are still wide-spread and well accepted by many service providers and users alike, several short-comings of this mechanism exist: Users tend to create unsafe passwords, forget passwords or use the same passwords for several applications [e.g., 20, 21, 46, 51]. Thus, a lot of research is done to develop and evaluate new forms of authentication technologies [21, 22, 36]. These include for example token-based solutions or graphical passwords [44].

© Springer International Publishing AG 2017
T. Tryfonas (Ed.): HAS 2017, LNCS 10292, pp. 265–283, 2017.
DOI: 10.1007/978-3-319-58460-7_18

The increasing availability of different types of sensors even in mobile devices such as smartphones also made it possible to use biometric authentication technologies. Biometric authentication relies on the recognition of either physical characteristics, like fingerprint, hand geometry, iris, retina, facial characteristics and DNA, or behavioral characteristics, e.g., signatures, keystroke dynamics or voice (which can also be classified as physical treat) [38]. The research in this area however often focuses on the technical aspects of implementing those technologies. Still, user perceptions and user acceptance are not necessarily in line with technical security or robustness of different technologies [2, 5, 18, 23]. The objective of this research was to explore user perceptions concerning security, preference, usage intention, effort, cost-benefit ratio, expected usage problems and privacy concerns using different forms of biometric and non-biometric authentication schemes. The first two research questions therefore were: "How do user perceptions of the interaction with different authentication schemes differ? What are the reasons for users' perceptions and preferences?"

We compared eight different authentication schemes, namely text password and graphical password as well as gesture, fingerprint, face, speech and ear shape recognition in a laboratory study with thirty-five participants. Each participant tested and evaluated each authentication scheme. In a final questionnaire and short interview the participants were asked to rate the tested schemes against each other and provide reasons for their preferences. The interaction with the authentication schemes was tested in a simulation to avoid external influences such as different levels of maturity or different interfaces. Furthermore, we aimed to protect our participants' data.

In context with the study design we were interested in whether the simulation "worked" in that participants didn't see through it. We were also interested in our participants' feedback and in possible ways to further improve the study design. Therefore the third and fourth research questions were: "Does the simulation work? How can the study design be improved further?"

We found that the text password, fingerprint recognition and iris recognition were the most preferred authentication schemes with our participants. The most reported reasons for preferring the biometric schemes fingerprint and iris recognition were the high perceived security due to the uniqueness of the feature and the ease of use. The text password however was not only preferred because of familiarity and perceived ease of use as well. Privacy aspects also played a major role. Several participants stated to prefer text passwords because no personal information had to be given away and couldn't be lifted or stolen. The least liked schemes were ear shape recognition, gesture recognition and the graphical password. Whereas the ear shape recognition was rated as impractical and effortful, participants thought the gesture recognition could be easily copied. The most likely cause for the negative rating of the graphical password were problems with the implementation. Overall, our results indicate that there might be two user groups that either prefer the password due to privacy concerns or biometrics due to the perceived security of using a unique feature for authentication. Earlier research suggests that user preference could further be influenced by context (e.g. newsletter vs. bank account) and familiarity with or knowledge about biometric vs. non-biometric schemes. Future research should address these questions that could have major implications for decision-makers choosing authentication schemes for their systems and services.

2 Related Work

O'Gorman [35] provided an extensive comparison of several knowledge-based, token-based and biometric authentication schemes in terms of security against different kinds of attacks, potential keyspace and entropy, host-side security and also some usability aspects like usage convenience, false nonmatch and false match rates. However, he did not compare the authentication schemes in an empirical study, but partly relied on individual empirical results from previous studies utilizing different study designs and partly based his evaluations merely on theoretical considerations. Bonneau et al. [7] chose a similar approach for rating a broad range of authentication schemes according to several security, usability and deployability criteria. An early literature review about the usability and security of alphanumeric and graphical passwords, token-based and biometric authentication procedures was conducted in 2004 by Sasse [39]. Furthermore, a literature review concerning the security and usability of several biometric authentication schemes can be found at Mayron et al. [34].

Some researchers compared the perceived security, acceptance and usability for a small range of authentication schemes. Bhagavatula et al. [5], for example, focused on smartphone authentication via Android's facial recognition system "Face Unlock" and Apple's fingerprint-based system "Touch ID". Compared to the traditional PIN authentication, two-thirds of survey participants who already used Face Unlock considered it to be more secure. Similar perceptions were found for users of Touch ID. In a corresponding lab study by Bhagavatula et al., seven out of ten participants ranked Face Unlock as their last or second last favored authentication scheme. Touch ID was preferred by six participants, whereas the remaining four described it as their least favorite scheme. Tari et al. [45] assessed the perceived and real vulnerability of the graphical password scheme "Passfaces" [37] to shoulder-surfing compared to alphanumeric passwords in a lab study, with participants trying to shoulder-surf while the experimenter authenticated himself. Both perceived and real shoulder-surfing vulnerability were rather high for Passfaces. Non-dictionary passwords were considered as less vulnerable, but were also found to be easier to shoulder-surf than dictionary passwords. As one of the first, Furnell and Evangelatos [19] conducted a focus group to investigate user perceptions, awareness and acceptance of different biometric authentication schemes, namely fingerprint, hand, signature, voice, keystroke, iris and retina recognition. Behavioral methods (keystroke, voice and signature analysis) were considered as least reliable, whereas fingerprint, iris and retina analysis received the highest ratings. However, iris and retina analysis scored lowest concerning how comfortable respondents would be to use the investigated schemes. Participants were also asked about their preference to use biometric compared to knowledge- and token-based schemes. More than half of the participants (61%) selected biometrics as their first preference, whereas 31% chose knowledge- and 10% token-based procedures.

Dörflinger et al. [14] conducted a focus group along with an online survey to assess the perceived security, goodness and usage intention for a wide range of authentication schemes, namely fingerprint recognition, 2D and 3D gesture recognition, retina scan, activity-based verification, speech recognition, face recognition and a recognition-based

graphical password. Participants in the focus group rated retina scan and fingerprint as most secure; the graphical password was considered as the least secure, followed by 3D and 2D gesture recognition. Surprisingly, participants were least likely to use retina scan for authentication in the future, which was also placed second to last in terms of goodness. Fingerprint, on the other hand, was the clear winner according usage intention and perceived goodness. In the online survey, fingerprint, iris and face recognition received the highest security ratings. In another focus group, Sieger and Möller [42] investigated gender differences concerning the perceived security of the same authentication schemes used by Dörflinger et al. [14], except for the graphical password. Though they focused on smartphone authentication, they received the same distribution of perceived security for the investigated schemes as Dörflinger and colleagues. They also found that female users tend to perceive all authentication schemes as being more secure, expect for speech recognition. Ben-Asher et al. [4] also did a survey and focus groups on the perceived security, acceptance, convenience and usage intention of several authentication schemes used on a smartphone. They included fingerprint recognition, gesture recognition, iris scan, voice recognition, face recognition, PIN/password and recognition of one's signature provided on a touch screen. Fingerprint was rated as most secure, followed by iris recognition and PIN/password. Gesture recognition was considered as least secure. Fingerprint and PIN/password also scored highest in terms of convenience, whereas participants clearly preferred PIN/password according to the likelihood of future usage.

While these are very interesting insights about user perceptions of different authentication schemes, the authors relied on more or less sophisticated demonstration of the particular authentication concepts [14] or mere textual presentation [42] and the participants did not actually use the described schemes. Further research is needed to investigate if the reported results can be replicated in a controlled setting based on actual interaction with the evaluated authentication schemes. We aim to contribute to filling that gap by using a controlled laboratory setting with a simulation design to avoid influences of different interfaces and stages of system maturity. Further, participants had the possibility to test and evaluate the actual interaction with eight different schemes. Most of the schemes chosen for this study have also been the object of investigation in the previous studies mentioned above to allow for a comparison of the results in terms of user perceptions.

3 Authentication Schemes

In the following section we describe findings of previous studies regarding user perceptions of the authentication schemes that were compared in the laboratory study.

3.1 Text Password

Text passwords are still the most common form of authentication. Among the shortcomings of text passwords researchers or users respectively list problems with the technical security [7], but also usability issues [27, 43]. The often mentioned poor

memorability leads users to apply work-around strategies such as choosing simple and/or guessable passwords, writing passwords on notes or re-using passwords for several accounts [3, 26, 40]. Even though not perfect, the analysis by Bonneau et al. revealed that text passwords still have benefits in terms of deployability and also some usability aspects such as "nothing-to-carry" and "easy-recovery-from-loss" [7]. Users in a survey by Ben-Asher et al. also attested the text password good values in terms of perceived security and convenience. Apart from that, the text password received the highest rating in terms of future intended use [4].

3.2 Graphical Password

Graphical passwords are an alternative to text passwords making use of the fact that people are better in memorizing pictures than words [1]. A range of graphical passwords exist that can broadly be divided into two categories. First, there are recognition-based techniques, where users e.g. have to recognize previously chosen pictures in a particular sequence among other distractors. Examples include Passfaces [37] or Déjà vu [16]. In recall-based variants users often have to recall and draw or click a certain pattern or sequence. Examples for this category are PassPoints [53] and Draw A Secret [28]. Further, some schemes use a combination of recognition-based and recall-based features. Advantages of graphical passwords include a better memorability [8, 16] compared to passwords and the possibility to increase the password space and therefore resistance to dictionary attacks, with a sufficiently large database. Also, some research suggests that graphical approaches might be more joyful for users [49]. On the other side, many graphical schemes come with an increased login-time compared to passwords or PINs [e.g. 31, 52] and, depending on the implementation, can be prone to shoulder-surfing.

3.3 Gesture Recognition

Gesture recognition can either be a non-biometric or a biometric authentication scheme depending on whether one's characteristic dynamics of completing the gesture are measured. Further, 2D gestures e.g. on a touch-screen as well as 3D gestures made in free air in front of a sensor can be used for authentication. In the focus groups conducted by Dörflinger, 2D gestures were rated better and more secure by the participants than 3D gestures. Also, the intention to use 2D gestures was higher [17]. Similar results were found by Sieger and Möller [42]. However, gesture detection in general only received very low ratings in the study by Ben-Asher [4]. User reactions is a study by Trewin et al. were mixed [47].

3.4 Biometric Authentication

The following procedures belong to the group of biometric authentication schemes. After Riley et al. [38] biometric authentication is defined as "the process of establishing an individual's identity through measurable characteristics of their behaviour, anatomy

or physiology." Biometric technologies are spreading and already find application in the governmental as well as in private sectors [38]. Whereas some researchers view biometrics as an advantageous approach because they confirm the actual presence of the legitimate user and apply characteristics that cannot be lost, forgotten or stolen, others raise concerns. Critics comprise the inability of a certain percentage of people to authenticate via biometrics, the problems arising for recovery from loss, and privacy issues [12, 46]. For example, in a laboratory study Toledano et al. [46] found that privacy concerns negatively affected confidence in biometrics. In focus groups conducted by Coventry et al. [13] privacy concerns were also raised as a problematic issue. Further, some researchers completely dismiss biometric authentication such as fingerprint because the features used are not per se secret and could be "lifted" [41].

Fingerprint Recognition. Fingerprint authentication is one of the most spread biometric authentication schemes, well-known by users due to the use in films, law enforcement and travel documents. It is also popular because of its high accuracy [32], maturity [12] and relatively low cost of acquisition devices [3]. In several user studies fingerprint recognition was rated as very secure and usable by the participants. For example, in focus groups conducted by Dörflinger et al. [17] fingerprint authentication received the highest acceptance and second highest security ratings compared to other biometric authentication technologies. In a survey by Jones et al. [29], participants perceived fingerprint authentication to be the most suitable biometric authentication technology for the financial and health care area. In a lab study by Holz and Bentley [24], participants experienced an increased sense of security when using fingering authentication in place of passwords to protect their e-mail account. Participants in a survey-based field study by Mare et al. [33] liked fingerprint authentication mainly because it was quick, even if they sometimes encountered failures with the sensors. Results from another survey by Cherapau et al. [10] suggest that besides its speed, participants value the convenience and ease of use of iPhones Touch ID fingerprint authentication. More than half of the participants also perceived it as secure. However, some participants also expressed concerns regarding the privacy of their provided fingerprint, due to uncertainty of whether Apple stores their fingerprints locally or somewhere else. Similar concerns were reported by participants in a survey conducted by De Luca et al. [15].

Face Recognition. Compared to the relatively long-established fingerprint recognition, face recognition is a rather new authentication solution [27]. However, it has recently gained publicity through the implementation of "Face Unlock" in Android phones. Reported user perceptions of this authentication scheme vary across studies: Results from a survey combined with focus groups by Ben-Asher et al. [4], as well as focus groups conducted by Dörflinger et al. [17] suggest a relatively low acceptance and usability of face recognition. A survey conducted by De Luca et al. [15] indicates a problem with perceived security for Android's Face Unlock, along with usability issues like low speed and lack of convenience concerning the correct placement of the smartphone for face scanning. Some participants also mentioned social awkwardness as one factor for not using Face Unlock, due to the fear of looking like they were taking selfies when scanning their face. Participants in a lab study by Bhagavatula et al. [5]

expressed concerns about attackers using a photograph to fool the face recognition system. However, other study results suggest high values for acceptance [47] and perceived security [5].

Iris Recognition. Most users have at least heard about iris recognition as an authentication scheme or seen its application in a movie [4]. Nonetheless, some users express concerns about this authentication approach, including reliability, health issues or misuse of their personal data, for example in a lab study conducted by Tassabehji and Kamala [44]. This is in line with results from another lab study by Crawford and Renaud [14], who found a low acceptance rate for iris recognition. But there are also positive statements from survey and focus group participants [4] in terms of acceptance or usage intention for iris recognition.

Speech Recognition. The recognition of speech can rely on both, behavioral biometric characteristics (i.e. speech pattern) and physiological characteristics (i.e. the individual sound of one's voice). Like for face recognition, users differ in their evaluation of speech recognition as an authentication solution. Some survey studies indicate high values for perceived security and future usage intention [11], but at the same time, results from other survey [4] or laboratory studies [48] suggest relatively low levels of acceptance, and low perceived security values [19].

Ear Shape Recognition. One of the first to investigate ears for identification was Iannarelli [26] who found that all of the more than 10,000 analyzed ears were distinguishable and thus ears provided sufficient unique properties to be used as a biometric. The recognition process is similar to facial recognition with 2D images or 3D models of the ear and does not need direct interaction [50]. Although ear shape recognition is seen as a promising approach by some researchers [25, 40, 50] the literature on the usability or security perception of ear shape recognition seems scarce. Problems might comprise ears covered by hair or hats and religious concerns to uncover ears for authentication [40].

4 Method

In the laboratory study thirty-five participants used and evaluated the eight simulated authentication technologies described above in a within-subject design. The text password as a classical authentication mechanism served as a baseline, whereas the remaining seven technologies were tested in a randomized order. The participants were asked to answer questions concerning the perceived security, effort and cost-benefit ratio, as well as expected usage problems and intention to use the authentication scheme in the future after using each scheme. The preference was rated after testing all schemes, along with possible privacy concerns associated with the authentication procedures.

4.1 Participants

The thirty-five participants that took part in the study were German undergraduates studying either psychology (29) or psychology in IT (6). Eleven participants were male, 24 female. Age ranged between 19 and 47 years with a mean of 23.09 (SD = 5.38).

About half of the participants (17 out of 35) have never used biometric authentication technologies before. All participants completed the study, there were no drop-outs. The participation was compensated with course credit.

4.2 Procedure

After the reception participants were asked to sit in front of a workstation used to simulate the different authentication schemes. The apparatus used for the simulation included an eye and facial expression tracking system called "FaceLAB"[1], a microphone and a built-in fingerprint sensor of a Sony VAIO notebook. The face, iris and ear shape recognition were simulated with the help of the FaceLAB system. For speech recognition, the participant was holding the microphone while saying a given password. We implemented a graphical password similar to PassPoints, where people have to click on predefined areas on a picture in a certain order to authenticate [53]. This procedure dates back to one of the first graphical schemes implemented in 1996, the so-called Blonder scheme [6]. The gesture recognition was implemented as a form of pattern recognition similar to the one used by "SoftKinetic"[2] for the PlayStation. The gesture was completed by moving a pointed finger in front of the FaceLAB camera in the form of the symbol for infinity (∞). Authentication was successful if the correct gesture was shown independent of individual dynamics.

The participant's workstation included two monitors. To one monitor the FaceLAB system was connected, the other monitor displayed instructions on the current authentication task. For reasons of data protection and privacy no biometric data was actually collected or stored. For the simulation, the participants' monitors were remotely controlled by the instructor. The participants' screens were duplicated and displayed on the screens of the instructor which were not visible for the participants. Participants were instead told that the data processing took place on the instructors' computer to provide a credible explanation for the connection between the computers. The experimental set-up is shown in Fig. 1.

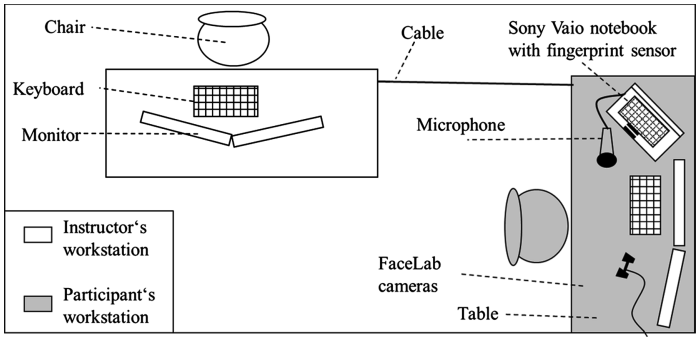

Fig. 1. Illustration of the experimental setup

[1] http://www.seeingmachines.com.

[2] https://www.softkinetic.com/products.

Before attending the main task, participants were told that several systems needed to be calibrated beforehand to be able to accurately authenticate the participants during the main task. Again, this was only simulated, but done to allow for a realistic authentication process. Thus, a simulated calibration phase was done for fingerprint recognition, face recognition, iris recognition, speech recognition and ear shape recognition.

After this the participants received the instruction to authenticate with a given text password at their workstation. The instruction was displayed on the screen. The familiar text password served as a baseline and to familiarize people with the procedure. After typing the correct password the participants received textual feedback on their screen indicating the authentication was successful. Participants were then asked to answer several questions on the authentication procedure based on a 5-point-Likert scale with 1 = strongly disagree and 5 = strongly agree, namely:

- Perceived security: "I think this authentication scheme is very secure, that is, it protects me against attacks."
- Expected problems: "I think the use of this authentication scheme generally causes no problems."
- Perceived effort: "How do you rate the effort for using this authentication scheme?" (based on a 5-point Likert-scale with 1 = very low and 5 = very high).
- Perceived cost-benefit ratio: "In my opinion, the effort exceeds the gained benefits for this authentication scheme."
- Intention to use: "If I had the possibility, I would use this authentication scheme."

Afterwards, the procedure was repeated with the other seven authentication schemes in a randomized order. Whenever the instructions were followed correctly, the participants received the "successful authentication"-message on their screen. Questions concerning the instructions were answered, in case of questions concerning technical features or functionality participants just received a general reassuring sentence such as "It works out fine" or "I can see on my computer that the data is processed correctly". After the completion of all authentication schemes participants received some final questions comparing all procedures used:

- Preference: "Please arrange the following authentication schemes according to how much you would like to use them, if all of them were available to you." (based on a ranking from 1 = most preferred to 8 = least preferred)
- Privacy concerns: "I have concerns to disclose the following data for usage of an authentication scheme." (based on a 5-point-Likert scale with 1 = strongly disagree and 5 = strongly agree)

The final part of the study was a half-structured interview asking for the reasons of why people preferred or not preferred certain schemes and why people perceived some procedure as more secure than others. Furthermore, some control variables such as age, gender, familiarity with biometrics and further comments were collected. The last part was the debriefing of the participants. They were told that all authentication schemes were simulated and that no data was stored or processed. Participants were then asked whether they saw through the simulation, and if yes, why that was the case. The participants were finally thanked for their participation, accredited with course credit and provided with contact information should any further questions arise later.

5 Results

In the following section the quantitative results of the questionnaires are presented along with the qualitative results from the interviews. We first describe the participants' perception of the authentication schemes, followed by an evaluation of the study design.

5.1 Preference

The results revealed that most participants preferred to authenticate via text password (11 out of 35), fingerprint (10 out of 35) or iris recognition (9 out of 35). Participants mostly appreciated text passwords due to habit, simplicity and protection of their personal data, for example:

- "I prefer the password, simply out of habit. I suppose it is not the most secure authentication scheme, but I haven't had any negative experiences with it and it is not exactly complex."
- "The question was which scheme I would mostly like to use and I think iris or face recognition are the best schemes, but I just don't want to disclose those [data], hence I chose the password."
- "I know it works well and with a good password you can protect yourself without disclosing personal information. This way, if your account is hacked, it is 'just' your account and not also your fingerprint."

Biometric authentication technologies, on the other hand, were preferred because they were seen as secure and simple and due to the uniqueness of the feature:

- "For me, it is very secure. Our iris is very…everyone has a special iris. It is very unique. Fingerprint is unique and iris too."
- "I think it is exiting, I liked that you could unlock the system with your fingerprint, because only I have this fingerprint. […] and I don't forget that like a password."
- "It is relatively secure, the eye is unique and it is simple once you have scanned it initially. You know it from movies."

The overall rating of the authentication schemes can be found in Fig. 2.

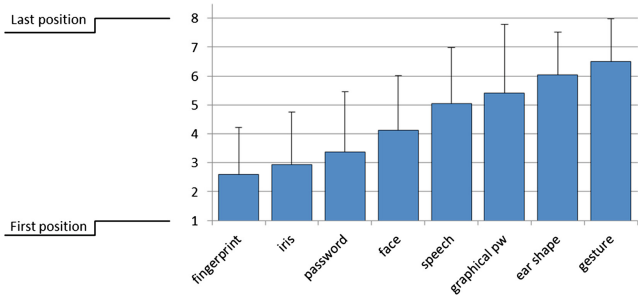

Fig. 2. Preference rating of all authentication schemes; low values indicating high preference

The least popular authentication technologies were the graphical password as well as gesture and ear shape recognition. The negative evaluation of the graphical password is likely to be caused by the rather imperfect technical implementation of the graphical password that manifested itself in the change of the mouse courser every time the mouse was placed in the correct area of the authenticating picture. Another reason for the negative evaluation was that the graphical password and the gesture recognition were viewed as easily copiable and therefore less secure:

- "In my opinion this can be fastest broken through guessing without knowing it."
- "Because of someone knows the gesture he could easily authenticate himself, I would say."

The ear shape recognition was seen as impractical and effortful:

- "I think the ear shape recognition was pointless. […] if you would employ it in daily life and had to turn your head every time…concerning the practicability and compatibility, I'm not such a great fan."
- "Because I think it's inefficient, it is impractical and I would not be keen to use it."

5.2 Perceived Security

Although there were no significant differences between the authentication technologies concerning the perceived security ($F(7, 238) = 0.48$, $p > .05$; see Fig. 3), sixteen out of thirty-five participants rated fingerprint as the most secure technology. The main reasons for this were uniqueness of the authentication feature as well as protection against forgery:

- "Fingerprint is most secure. Iris and face recognition are on the same level. Simply in terms of security…because…fingerprint is unique. Because as far as I now a fingerprint can't be replicated. And the other schemes all provide some opportunity for attacks. And I think the fingerprint scan is difficult to crack from outside the system, you have to get into the system somehow to access the data and copy them."
- "The probability for someone to have the same fingerprint is one billion or so. You can spoof the face with a photo or something like that, but fingerprint is hard [to spoof]."

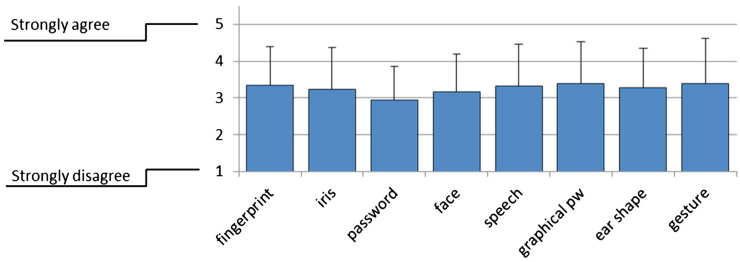

Fig. 3. Perceived security of the tested authentication schemes

Text passwords were also considered as secure "as long as they are applied correctly", i.e. in accordance with common password guidelines:

- "The password is most secure if you apply it correctly. Biometric characteristics can be forged easily, passwords are relatively complex, there are more units to vary."

5.3 Privacy Concerns

However, fingerprint is also the authentication feature for which most participants have concerns to reveal their data, followed by face and iris recognition (differences were significant with $F(4.1, 142.7) = 11.74$, $p < .001$, partial $\eta^2 = 0.25$, see Fig. 4).

The participants also mentioned these concerns in the interviews:

- "It depends on in whose hands it is, if I authenticate myself via fingerprint when entering a country or to identify a delinquent, then I think it's secure, but I still have a bad feeling to disclose this data to the state because I don't know how it is protected."
- "I think it is questionable because the eye is scanned offhandedly. One is just not as familiar with iris recognition as with fingerprint and that stokes fear about digitalization and the 'transparent citizen'."

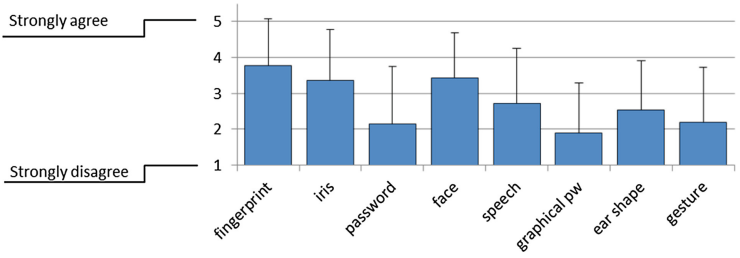

Fig. 4. User concerns to reveal the data necessary for the particular authentication scheme

5.4 Perceived Effort

There were no significant differences concerning the perceived effort for using the authentication schemes ($F(7, 238) = 1.39$, $p > .05$). Overall, participants expected the effort for using the schemes to be relatively low (mean ranged between 2.2 and 2.5). Accordingly, on average participants rated the cost-benefit-ratio for using the authentication schemes as positive (mean ranged between 1.9 and 2.1). Again, there were no significant differences between the eight authentication schemes ($F(4.7, 160.5) = 0.89$, $p > .05$).

5.5 Expected Problems

Participants mainly expect to have problems with the ear shape and face recognition, whereas the other authentication schemes are expected to perform relatively equal, on a

moderate, but slightly positive level (see Fig. 5). The differences in the expected occurrence of problems were significant with $F(4.7, 159.5) = 2.91$, $p < .05$, partial $\eta^2 = 0.08$.

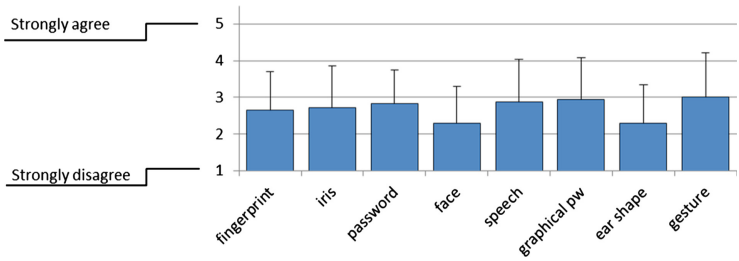

Fig. 5. Expected problems during the usage

5.6 Intention to Use

Although there were also no significant differences in the intention to use the authentication schemes in the future ($F(7, 238) = 1.05$, $p > .05$), the text password still received the highest value, i.e. on average, participants are most inclined to use the text password if they could freely choose between all considered authentication schemes (mean ranged between 2.9 and 3.6).

5.7 Simulation

The majority of participants did not see through the simulation of the authentication schemes. After having been informed about the procedure 22 participants stated they had not been suspicious about the implementation of the authentication schemes. For eight participants, the classification was ambiguous as they mentioned minor concerns only after being informed. Five participants either raised questions during the experiment or clearly stated to have had suspicions after being informed. Some participants stated the authentication process was too "smooth" to be realistic. Of the five, four also had personal experience with biometric authentication.

6 Discussion

The results revealed that even though alternatives are spreading the familiar text password is still popular as authentication method. The text password was the most commonly mentioned preference in the interviews and also ranged among the top three schemes in the list of average preference positions. In accordance with some previous studies fingerprint and iris recognition received the highest values among the biometric schemes. For example, in a survey by Furnell and Evangelatos [19] fingerprint and iris scan were rated the most reliable and Karatzouni et al. [30] found fingerprint to be the most popular choice for the implementation of biometrics on smartphones. Interestingly, none of the schemes investigated in our study differed significantly in terms of

their perceived security. Thus, the reasons for the lower ranking of other biometric schemes such as face, speech or ear shape recognition seem to lie in other areas. The rating of expected problems reveals that users expect the face and ear shape recognition to cause more problems than other schemes what might be an explanation. Further, several statements in the interviews indicate that people might feel uncomfortable using speech, face or ear shape recognition in the public. This finding of expected "social awkwardness" is in line with the results of De Luca et al. [15]. The higher ranking of fingerprint and iris recognition might also be connected to the finding that most of our participants who had used biometrics before, had experience with fingerprint recognition. In a survey by Jones et al. conducted in 2007 [29], the fingerprint also was the biometric scheme most participants were familiar with. It is to be expected that the familiarity with fingerprints even increased since then. Further, both fingerprint and iris recognition are among the more commonly used technologies in films, e.g. in crime movies. As a reason for her preference one participant even stated that she knew from films that the iris scan was easy to use and relatively secure.

Another interesting result is that the text password and biometric technologies seem to be preferred for different reasons. The text password is valued not only due to its familiarity but also because no unique, personal information has to be confided to the authentication system and therefore cannot be stolen by an attacker. However, biometrics seem to be valued mainly due to this exact fact. Participants mostly named the uniqueness and unforgeability of the feature as a reason for using biometrics. This leads to the question of whether different user groups exist preferring either the text password due to privacy concerns or biometric technologies for perceived security reasons. The assumption of different user preferences is supported by results of other studies showing that people seem to have complex, somewhat dichotomous opinions about biometrics [9, 38]. In connection with this question one should also consider possible influences of variables that have not yet been tested in the current laboratory study. As mentioned above, the familiarity with biometrics, both personal experience and the familiarity from movies, might influence their assessment. Apart from that, Heckle, Patrick and Ozok [23] found that users were more comfortable using biometrics for personal versus corporate purchases in an online shopping context. The survey results of Jones et al. [29] revealed that in the financial domain the text password was rated as slightly more acceptable than a fingerprint scan, whereas the order changed in the health care sector. In the retail domain again passwords were rated as more appropriate than fingerprint and other biometrics. These results indicate that the authentication context might affect user preference for biometrics versus passwords as well. Future research should address these questions. Due to the short-comings of the implementation of the graphical password it remains open whether the assumption of different user groups is only valid for text passwords versus biometrics or for knowledge-based procedures in general. This question could be addressed in future studies as well.

It is noticeable that the perceived effort did not differ between the different schemes. A reason for this result might be that all our simulated schemes provided a similar interface and were implemented with a zero-error rate to avoid influences of a particular problem on the evaluation of the interaction. On the one hand, the results indicate that the simulation was successful in avoiding theses influences on the participants' assessment. On the other hand, the assessments in a real-life environment with current

implementations of the technologies might differ a lot. It is to be expected that errors e.g. due to hand lotion on fingers when using the fingerprint sensor affect users' evaluation of the system. Therefore, to increase the external validity of the results in this regard, future studies should address the problems and error rates of current solutions in the study design. Overall, the simulation worked well for the majority of the participants. Nearly two thirds of the participants were convinced of the functionality of the tested authentication schemes, further eight expressed questions or doubt only after being informed about the simulation. Still, one has to take into account that most of the users were non-experts in terms of information technology and biometric authentication schemes. Only half of the participants had used some form of biometric authentication before. Furthermore, the imperfect implementation of the graphical password might have caused distortions in the participants' assessments. Thus, the inclusion of actual problems and error rates of current solutions as well as the redesign of the interfaces is expected to lead to a further improvement of the simulation in future studies.

6.1 Limitations

Despite the aspects discussed in the context of the study design the research had the following limitations: First, all participants were undergraduate students. Therefore, the sample has been skewed in terms of age, education and technical affinity. About half of the participants already had personal experience with some form of biometrics. This might have been affected the ratings compared to participants who had no personal experience with biometric authentication schemes. Second, the relatively homogenous sample only consisted of thirty-five participants. A larger and more heterogeneous sample would increase the external validity of the results. Third, the tested authentication schemes included several biometric schemes, but for example only one graphical scheme. Token-based schemes were not tested at all. Thus, the inclusion of further knowledge-based and token-based schemes would lead to a more balanced approach. One indication for this effect is that all authentication schemes received a similar rating concerning the expected effort and the perceived cost-benefit ratio. To clarify the influence of the study design on these results it would have been interesting to have the participants provide reasons for their assessments. To increase the degree of realism a future study design should take real world problems and error-rates of the particular authentication schemes into account.

6.2 Conclusion

Concluding, the current research provided valuable insights in user perceptions concerning a broad range of authentication technologies. Whereas some findings were in line with previous studies, such as the high user preference for fingerprint recognition among biometrics, others were a bit surprising in comparison with earlier findings, e.g. the low rating of face recognition or the graphical password. The rating of face recognition can be explained with usage problems expected by the participants. The bad rating of the graphical password is most likely caused by short-comings in the implementation. The combination of user ratings and explanations led to the assumption of different user

groups preferring either the password due to privacy concerns or biometrics due to the perceived security of the unique feature used to authenticate. This hypothesis needs to be analyzed further in the future, together with further influencing variables. The simulated study design in general proved effective to compare different authentication schemes in a controlled setting while protecting the data and privacy of our participants. However, to improve the external validity and persuasive power of the simulation, its limitations should be addressed in future studies.

Acknowledgments. This work was supported by the German Federal Ministry of Education and Research (BMBF) as well as by the Hessen State Ministry for Higher Education, Research and the Arts (HMWK) within CRISP. Furthermore, the research reported in this paper has been supported by the German Federal Ministry of Education and Research (BMBF) within MoPPa.

References

1. Abdullah, M.D.H., Abdullah, A.H., Ithnin, N., Mammi, H.K.: Towards identifying usability and security features of graphical password in knowledge based authentication technique. In: Second Asia International Conference on Modelling & Simulation (AMS), pp. 396–403. IEEE Press, New York (2008). doi:10.1109/AMS.2008.136
2. Al-Harby, F., Qahwaji, R., Kamala, M.: The feasibility of biometrics authentication in e-commerce: user acceptance. In: IADIS International Conference WWW/Internet (2008)
3. Alonso-Fernandez, F., Bigun, J., Fierrez, J., Fronthaler, H., Kollreider, K., Ortega-Garcia, J.: Fingerprint Recognition. In: Petrovska-Delacrétaz, D., Chollet, G., Dorizzi, B. (eds.) Guide to Biometric Reference Systems and Performance Evaluation, pp. 51–88. Springer, London (2009)
4. Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., Möller, S.: On the need for different security methods on mobile phones. In: The 13th International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI 2011), pp. 465–473. ACM Press, New York (2011). doi:10.1145/2037373.2037442
5. Bhagavatula, C., Ur, B., Iacovino, K., Kywe, S.M., Cranor, L.F., Savvides, M.: Biometric authentication on iphone and android: usability, perceptions, and influences on adoption. In: Workshop on Usable Security (2015). doi:10.14722/usec.2015.23003
6. Blonder, G.: Graphical password. United States Patent 5559961, Lucent Technologies, Inc., Murray Hill (1996)
7. Bonneau, J., Herley, C., van Oorschot, P.C., Stajano, F.: The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In: IEEE Symposium on Security and Privacy, pp. 553–567. IEEE Press, New York (2012). doi.10.1109/SP.2012.44
8. Brostoff, S., Sasse, M.A.: Are passfaces more usable than passwords: a field trial investigation. In: McDonald, S., Waern, Y., Cockton, G. (eds.) People and Computers XIV – Usability or Else: Proceedings of HCI, pp. 405–422. Springer, Sunderland (2000). doi:10.1007/978-1-4471-0515-2_27
9. Chen, K.-Y., Chang, M.-L.: User acceptance of 'near field communication' mobile phone service: an investigation based on the 'unified theory of acceptance and use of technology' model. Serv. Ind. J. **33**, 609–623 (2013). doi:10.1080/02642069.2011.622369
10. Cherapau, I., Muslukhov, I., Asanka, N., Beznosov, K.: On the impact of touch ID on iPhone passcodes. In: Symposium on Usable Privacy and Security (SOUPS), pp. 257–276 (2016)

11. Clarke, N., Furnell, S., Rodwell, P., Reynolds, P.: Acceptance of subscriber authentication methods for mobile telephony devices. Comput. Secur. **21**, 220–228 (2002). doi:10.1016/S0167-4048(02)00304-8
12. Clausen, S.: A single-line AC capacitive fingerprint swipe sensor. In: Ratha, N.K., Govindaraju, V. (eds.) Advances in Biometrics. Sensors, Algorithms and Systems, pp. 49–62. Springer, London (2008). doi:10.1007/978-1-84628-921-7_3
13. Coventry, L., DeAngeli, A., Johnson, G.: Honest it's me! Self service verification. In: ACM CHI Workshop on Human-Computer Interaction and Security Systems (2003)
14. Crawford, H., Renaud, K.: Understanding user perceptions of transparent authentication on a mobile device. J. Trust Manage. **1**, 1–7 (2014). doi:10.1186/2196-064X-1-7
15. De Luca, A., Hang, A., von Zezschwitz, E., Hussmann, H.: I feel like I'm taking selfies all day! Understanding biometric authentication on smartphones. In: Conference on Human Factors in Computing Systems, pp. 1411–1414. ACM Press, New York (2015). doi:10.1145/2702123.2702141
16. Dhamija, R., Perrig, A.: Déjà Vu: a user study using images for authentication. In: The 9th USENIX Security Symposium, p. 4. The USENIX Association, Berkeley (2000)
17. Dörflinger, T., Voth, A., Krämer, J., Fromm, R.: "My smartphone is a safe!" The user's point of view regarding novel authentication methods and gradual security levels on smartphones. In: Katsikas, S.K., Samarati, P. (eds.) International Conference on Security and Cryptography (SECRYPT), pp. 155–164. IEEE Press, New York (2010)
18. Eze, U.C., Gan, G.G.G., Ademu, J., Tella, S.A.: Modelling user trust and mobile payment adoption: a conceptual Framework. Commun. IBIMA **3**, 224–231 (2008)
19. Furnell, S., Evangelatos, K.: Public awareness and perceptions of biometrics. Comput. Fraud Secur. **1**, 8–13 (2007). doi:10.1016/S1361-3723(07)70006-4
20. Grawemeyer, B., Johnson, H.: Using and managing multiple passwords: a week to a view. Interact. Comput. **23**, 256–267 (2011). doi:10.1016/j.intcom.2011.03.007
21. Harbach, M., Fahl, S., Rieger, M., Smith, M.: On the acceptance of privacy-preserving authentication technology: the curious case of national identity cards. In: Cristofaro, E., Wright, M. (eds.) PETS 2013. LNCS, vol. 7981, pp. 245–264. Springer, Heidelberg (2013). doi:10.1007/978-3-642-39077-7_13
22. Harbach, M., von Zezschwitz, E., Fichtner, A., De Luca, A., Smith, M.: It's a hard lock life: a field study of smartphone (un) locking behavior and risk perception. In: Symposium on Usable Privacy and Security (SOUPS), pp. 213–230 (2014)
23. Heckle, R.-R., Patrick, A.S., Ozok, A.: Perception and acceptance of fingerprint biometric technology. In: The 3rd Symposium on Usable Privacy and Security, pp. 153–154 (2007). doi:10.1145/1280680.1280704
24. Holz, C., Bentley, F.R.: On-demand biometrics: fast cross-device authentication. In: CHI Conference on Human Factors in Computing Systems, pp. 3761–3766. ACM Press, New York (2016). doi:10.1145/2858036.2858139
25. Holz, C., Buthpitiya, S., Knaust, M.: Bodyprint: biometric user identification on mobile devices using the capacitive touchscreen to scan body parts. In: The 33rd Annual ACM Conference on Human Factors in Computing Systems, pp. 3011–3014. ACM Press, New York (2015)
26. Iannarelli, A.V.: Ear Identification. Paramont Publishing Company, Paramount (1989)
27. International Civil Aviation Organization: Biometric Identification To Provide Enhanced Security And Speedier Border Clearance For Travelling Public (PIO 09/2003). http://www.icao.int/icao/en/nr/2003/pio200309.htm
28. Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D.: The design and analysis of graphical passwords. In: The 8th USENIX Security Symposium, p. 1. The USENIX Association, Berkeley (1999)

29. Jones, L.A., Anton, A.I., Earp, J.B.: Towards understanding user perceptions of authentication technologies. In: ACM Workshop on Privacy in Electronic Society, pp. 91–98. ACM Press, New York (2007). doi:10.1145/1314333.1314352
30. Karatzouni, S., Furnell, S.M., Clarke, N.L., Botha, R.A.: Perceptions of user authentication on mobile devices. In: International Conference for Internet Technology and Secured Transactions (ICITST), IEEE Press, New York (2011)
31. Ma, Y., Feng, J.: Evaluating usability of three authentication methods in web-based application. In: Ninth International Conference on Software Engineering Research, Management and Applications (SERA), pp. 81–88. IEEE Press, New York (2011). doi:10.1109/SERA.2011.18
32. Maio, D., Maltoni, D., Capelli, R., Wayman, J.L., Jain, A.K.: FVC2000: fingerprint verification competition. IEEE Trans. Pattern Anal. Mach. Intell. **24**, 402–412 (2002)
33. Mare, S., Baker, M., Gummeson, J.: A study of authentication in daily life. In: Symposium on Usable Privacy and Security (SOUPS), pp. 189–206 (2016)
34. Mayron, L.M., Hausawi, Y., Bahr, G.S.: Secure, usable biometric authentication systems. In: Stephanidis, C., Antona, M. (eds.) UAHCI 2013. LNCS, vol. 8009, pp. 195–204. Springer, Heidelberg (2013). doi:10.1007/978-3-642-39188-0_21
35. O'Gorman, L.: Comparing passwords, tokens, and biometrics for user authentication. Proc. IEEE **91**, 2021–2040 (2003). doi:10.1109/JPROC.2003.819611. IEEE, New York
36. Paul, C.L., Morse, E., Zhang, A., Choong, Y.-Y., Theofanos, M.: A field study of user behavior and perceptions in smartcard authentication. In: Campos, P., Graham, N., Jorge, J., Nunes, N., Palanque, P., Winckler, M. (eds.) INTERACT 2011. LNCS, vol. 6949, pp. 1–17. Springer, Heidelberg (2011). doi:10.1007/978-3-642-23768-3_1
37. Real User Corporation, Passfaces TM. http//:www.realuser.com
38. Riley, C., Buckner, K., Johnson, G., Benyon, D.: Culture & biometrics: regional differences in the perception of biometric authentication technologies. AI Soc. **24**, 295–306 (2009). doi:10.1007/s00146-009-0218-1
39. Sasse, M.A.: Usability and trust in information systems. In: Mansell, R., Collins, B. (eds.) Trust and Crime in Information Societies, pp. 319–348. Edward Elgar, Cheltenham (2005)
40. Scheuermann, D., Schwiderski-Grosche, S., Struif, B.: Usability of biometrics in relation to electronic signatures. Report, GMD-Forschungszentrum Informationstechnik (2000)
41. Schneier, B.: Secrets and Lies: Digital Security in a Networked World. Wiley, Hoboken (2000)
42. Sieger, H., Möller, S.: Gender differences in the perception of security of mobile phones. In: The 14th International Conference on Human-Computer Interaction with Mobile Devices and Services Companion, pp. 107–112. ACM Press, New York (2012). doi:10.1145/2371664.2371685
43. Stobert, E., Biddle, R.: Memory retrieval and graphical passwords. In: The Ninth Symposium on Usable Privacy and Security, Article 15. ACM Press, New York (2013). doi:10.1145/2501604.2501619
44. Tassabehji, R., Kamala, M.A.: Improving e-banking security with biometrics: modelling user attitudes and acceptance. In: The 3rd International Conference on New Technologies, Mobility and Security, pp. 110–115. IEEE Press, Piscataway (2009)
45. Tari, F., Ozok, A.A., Holden, S.H.: A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In: The Second Symposium on Usable Privacy and Security, pp. 56–66. ACM, New York (2006). doi:10.1145/1143120.1143128
46. Toledano, D.T., Pozo, R.F., Trapote, A.H., Gomez, L.H.: Usability evaluation of multi-modal biometric verification systems. Interact. Comput. **18**, 1101–1122 (2006). doi:10.1016/j.intcom.2006.01.004

47. Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K., Ben-David, S.: Biometric authentication on a mobile device: a study of user effort, error and task disruption. In: The 28th Annual Computer Security Applications Conference, pp. 159–168. ACM Press, New York (2012). doi:10.1145/2420950.2420976
48. Turner, C., Safar, J., Ramaswamy, K.: The effects of use on acceptance and trust in voice authentication technology. Proc. Hum. Factors Ergon. Soc. Annu. Meet. **50**, 718–722 (2006). doi:10.1177/154193120605000522
49. Von Zezschwitz, E., Koslow, A., De Luca, A., Hussmann, H.: Making graphic-based authentication secure against smudge attacks. In: The 2013 International Conference on Intelligent User Interfaces, pp. 277–286. ACM Press, New York (2013)
50. Yan, P., Bowyer, K.W.: Biometric recognition using 3D ear shape. IEEE Trans. Pattern Anal. Mach. Intell. **29**, 1297–1308 (2007). doi:10.1109/TPAMI.2007.1067
51. Wash, R., Rader, E., Berman, R., Wellmer, Z.: Understanding password choices: how frequently entered passwords are re-used across websites. In: Symposium on Usable Privacy and Security (SOUPS), pp. 175–188 (2016)
52. Weiss, R., De Luca, A.: PassShapes: utilizing stroke based authentication to increase password memorability. In: Proceedings of the 5th Nordic Conference on Human-Computer Interaction: Building Bridges, pp. 383–392. ACM Press, New York (2008). doi:10.1145/1463160.1463202
53. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., Memon, N.: Passpoints: design and longitudinal evaluation of a graphical password system. Int. J. Hum. Comput. Stud. **63**, 102–127 (2005). doi:10.1016/j.ijhcs.2005.04.010