Security vs. privacy? User preferences regarding text passwords and biometric authentication

Nina Gerber, Verena Zimmermann

Department of Human Sciences, Technische Universität Darmstadt

Abstract

Although text passwords suffer from several flaws, they are still wide-spread. Biometric authentication schemes are one possible alternative. However, previous study results suggest there might be two user groups preferring either knowledge-based or biometric authentication, due to different reasons. We conducted an online survey with 95 German participants to test this assumption. Our results provide evidence for the existence of two user groups, with preferences varying between different usage scenarios. Main reasons named for both methods are efficiency, security and habit, whereas privacy is another advantage provided by text passwords. Service providers should consider this diverging preferences in their decision to implement a particular authentication method.

1 Introduction

Although there is much empirical evidence for the weaknesses of password/username authentication solutions (Tari et al., 2006; Wimberly and Liebrock, 2011), text passwords continue to be the de facto standard in web-based service end-user authentication. This seems surprising, considering the fact that the shortcomings of passwords not only include several problems with the provided security, but also various usability flaws (Bonneau et al., 2015), many associated with their poor memorability (Stobert and Biddle, 2013). As a consequence, many users tend to choose simple and/or guessable passwords, write them down, share them or use the same password for different accounts (Inglesant and Sasse, 2010; Shen et al., 2016). One possible alternative to text passwords are biometric systems. 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) (Rodrigues and Santos, 2013). The introduction of Android face unlock and iPhone fingerprint recently has been the first deployment of biometric systems for end-users on a large scale (Bhagavatula et al., 2015). However,

Veröffentlicht durch die Gesellschaft für Informatik e. V. 2017 in
M. Burghardt, R. Wimmer, C. Wolff, C. Womser-Hacker (Hrsg.):
Mensch und Computer 2017 – Workshopband, 10.–13. September 2017, Regensburg.
 https://doi.org/10.18420/muc2017-ws05-0405

while some users embrace the new convenient alternative to text passwords, others seem to reject using biometric authentication schemes, mostly for privacy reasons (Toledano et al., 2006; Coventry et al., 2003).

As one of the first, Furnell and Evangelatos compared the users' perceptions, awareness and acceptance of different biometric authentication schemes in a survey (Furnell and Evangelatos, 2007). They did not focus on a specific device, but rather investigated the users' perceptions of biometric authentication schemes in general, as well as for different use cases, e.g., airport check-ins, online transactions, and login for PCs, laptops and cell phones. When asked about their preferences to use either biometric, knowledge- or token-based authentication schemes, more than half of the participants (61%) stated they would prefer to use biometric schemes, whereas 31% chose knowledge- and 10% token-based procedures. Biometric schemes (i.e. fingerprint, iris and retina scan) were also considered as most reliable. However, iris and retina scan received the lowest values when participants were asked how comfortable they would feel to use the investigated authentication schemes. This is in line with the results from a focus group conducted by Dörflinger et al. (Dörflinger et al., 2010), who found that although fingerprint and retina scan were considered as most secure for authenticating on a smartphone among several biometric and knowledge-based authentication schemes, participants were least likely to use retina scan for authentication purposes in the future. Fingerprint, on the other hand, was the clear winner regarding usage intention. Then again, the participants in a focus group and online survey conducted by Ben-Asher et al. (Ben-Asher et al., 2011) clearly preferred PIN/password to authenticate themselves on a smartphone. PIN/Password was also the authentication scheme that was considered as most convenient, together with fingerprint, which was further rated as most secure.

Although most of the studies described above focus on authentication on a smartphone, which might be evaluated differently than authenticating on a PC/laptop by the users, we also found evidence for this seemingly ambivalent perception of biometric technologies in a previously conducted laboratory study comparing different biometric and knowledge-based schemes for authenticating on a PC/laptop (Zimmermann and Gerber, in press): Eleven out of 35 participants preferred to authenticate via text password in the future, 10 preferred fingerprint and 9 iris recognition. Participants who preferred text passwords did this mainly out of habit and familiarity or for reasons of simplicity and protection of their personal data. Biometric authentication schemes were appreciated because they were seen as secure due to the uniqueness if the feature used for authentication (e.g., fingerprint or iris) and easy to use. These results suggest there might be two different user groups, either preferring text passwords for privacy reasons or biometric authentication due to the perceived security of using a unique feature for authentication.

Hence, we conducted an online survey with 95 participants to test whether users can indeed be assigned to one of the two groups preferring either knowledge-based authentication via text passwords or biometric authentication. Furthermore, we wanted to investigate the reasons for preferring knowledge-based or biometric authentication in more detail. Since results from a survey conducted by Jones et al. (Jones et al., 2007) indicate that the preference for knowledge-based vs. biometric authentication might be affected by the authentication context (with partic-

ipants preferring passwords in the financial and retail domain and fingerprint in the health care sector), we decided to consider this aspect as well.

2 Method

We conducted an online survey with 95 participants. All questionnaires were implemented in SoSci Survey (Leiner, 2016). All questions were presented in German. It took participants about 12 minutes to complete the whole survey. Participants were recruited via mailing lists and postings in social networks. The participants received no monetary compensation. Instead, one Amazon voucher á 75€ was drawn among all participants.

First, we provided a short explanation of text password and biometric authentication. Then we asked whether the participants preferred to authenticate via text password or biometric schemes or whether they had no preference at all. If the participants had chosen one authentication scheme above the other, they were prompted to provide reasons for their choice in an open answer format. This procedure was repeated for seven different usage scenarios, all referring to authentication on a notebook. The usage scenarios were presented in randomized order. Namely, we considered the following scenarios: (1) Online banking, (2) E-Mail encryption, (3) Social networks, (4) Online shops which are connected to one's bank account, (5) Cloud services, (6) E-Mail account, (7) Notebook unlocking.

For each scenario, participants had the opportunity to select "I do not use this service". At the end of the survey, participants were asked how important they felt it is to protect their data from third parties for the different usage scenarios. Finally, they were asked to provide demographic information.

A total of 129 participants completed the survey. For the analysis, all participants who reported to have no preference for either text passwords or biometric authentication (17, 13%) or to be unfamiliar with at least one of the services we asked about in the scenarios (17, 13%) were excluded. This leaves a final sample of 95 participants. Of these, 55 (57.9%) were female and 40 (42.1%) were male, ranging in age from 17 to 72 years (M=28.71, SD=11.88). About half of the participants (51, 54%) were students, 41 (43%) either part- or full time employees and 3 (3%) self-employed. Thirty-six (38%) participants had already used biometric authentication schemes and 11 (12%) had an IT-background.

3 Results

The open answers were analyzed following the Grounded Theory method (Mey and Mruck, 2010), i.e., we first conducted an open coding, which then served as basis for the formulation of categories. Finally, the participants' answers were assigned to the final categories. The categorization was conducted independently by two researchers. Differences in the categorization were solved afterwards through group discussion.

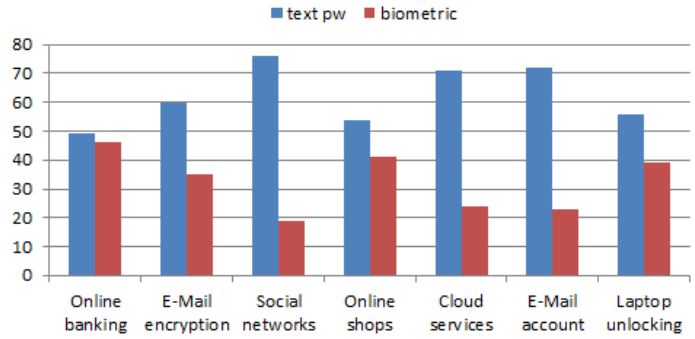

Figure 1: Number of participants preferring text password or biometric authentication for the different usage scenarios.

3.1 Overall preference

A total of 52 participants chose text passwords as their preferred authentication scheme, mainly for reasons of efficiency (33) and security (22). Biometric authentication schemes were preferred by 43 participants, again mostly due to high security (37) and efficiency (37). Participants who reported to have an IT-background did not differ from those without such a background regarding the overall usage preference. Not surprisingly, participants who were already using biometric authentication schemes were more likely to prefer these schemes ($\chi^2(1)=8.12$, $p<.01$).

3.2 Usage scenarios

Using McNemar tests for connected samples with Bonferroni correction, we found that the participants' overall preference differed significantly from the preference for authenticating for social network ($\chi^2(1)=19.20$, $p<.01$), cloud service ($\chi^2(1)=37.23$, $p<.01$) and e-mail accounts ($\chi^2(1)=48.08$, $p<.01$), with more participants preferring to authenticate via text passwords and less via biometric authentication schemes in all three scenarios, compared to their reported overall preference. No significant difference was found for the remaining usage scenarios. The preferences reported for the seven usage scenarios are displayed in Figure 1. Figure 2 displays how important it is for the participants to protect their data from third parties in the different usage scenarios.

3.2.1 Online banking

A total of 49 participants preferred to authenticate via text password for their online banking account, 46 preferred to use biometric authentication. Those preferring text passwords do this mainly out of habit (28), because they perceive text passwords as secure (19), they don't have to provide personal information (12) and they think text passwords are efficient (10). Biometric

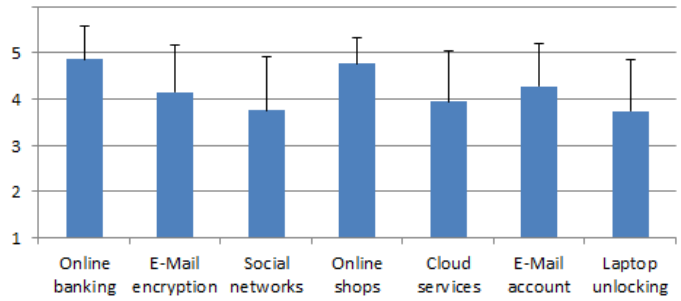

Figure 2: Importance to protect data from third parties, with 1=very unimportant and 5=very important.

authentication is preferred due to high perceived security (48), efficiency (13) and out of habit (12).

3.2.2 Online shops connected to one's bank account

Online shops which are connected to one's bank account are preferably accessed via text password by 54 and via biometric authentication by 41 participants. The main reasons for using text passwords were high perceived security (21) and privacy (17), followed by efficiency and habit (13, respectively). Like text passwords, biometrics were mostly preferred because of high security (41). Other reasons were efficiency (11) and habit (8).

3.2.3 Social network account

For accessing their social network accounts, 76 participants preferred to authenticate via text password and 19 via biometrics. Text passwords were preferred out of habit (29), as well as for reasons of privacy (26), efficiency (24) and security (22). Biometric authentication was chosen because it is considered as secure (11), efficient (9) and out of habit (7).

3.2.4 E-Mail account

For accessing their E-Mail accounts, 72 participants preferred to authenticate via text password and 23 via biometrics. Habit is the main reason for choosing text passwords to access one's e-mail account (35), followed by efficiency (27), security (23) and privacy protection (13). Biometrics were mainly chosen for their high security (14), their efficiency (9) and out of habit (6).

3.2.5 E-Mail encryption

Concerning e-mail encryption, 60 participants preferred authentication via text passwords and 35 via biometrics. Reasons for text password usage were habit (23), privacy protection (21), perceived security (17) and efficiency (11). Biometrics, on the other hand, were preferred because they were perceived as secure (29), efficient (12) and out of habit (7).

3.2.6 Cloud service account

Cloud services were preferably accessed via text password by 71 and via biometric authentication by 24 participants. Main reasons for using text passwords were habit (27), and privacy protection (23), followed by efficiency (19) and security (20). Participants who preferred biometrics did so because of it's high security (13) and efficiency (11).

3.2.7 Notebook unlocking

To unlock their notebook, 56 participants preferred to use text passwords and 39 biometric authentication. Again, text passwords were preferred because participants are used to them (19), perceive them as secure (15) and efficient (14). Biometrics were mainly chosen because they are perceived as efficient (24), secure (13) and out of habit (9).

4 Discussion

With roughly 50% preferring text passwords and biometric authentication schemes, respectively, our results provide evidence for the assumption of two different user groups. However, the main reasons reported by our participants to prefer text passwords did not concern privacy, as we had assumed, but related to its' efficiency and security. Interestingly, biometric authentication schemes were preferred for the same reasons. Compared to their overall preference, more participants preferred to use text passwords when authenticating for their accounts in social networks, cloud services, and their e-mail accounts. Since these use cases are typically among the ones performed most frequently by online users, it is possible that participants relied to a greater extend on their experiences with prior authentications when evaluating their preferred authentication method for these scenarios, compared to the other use cases. Indeed, many participants reported to prefer text passwords in these usage scenarios because they were accustomed to this procedure. Contrary to the reported overall preference, privacy seems to be an issue for the participants preferring text passwords in all usage scenarios except for unlocking one's notebook. Habit seems to be another important reason to prefer both authentication methods in all seven usage scenarios, besides efficiency and security. Hence, it is important to consider the concrete use case when investigating authentication preferences. Additionally, service providers should keep in mind that their users might be parted in two different groups of authentication types when deciding which authentication method they want to implement. To please the majority of their users, it may be necessary to implement both, knowledge-based and biometric authentication solutions and let the users choose their preferred authentication method. However, this might not always be possible, since some online services require particularly strong authentication. To please both user groups and provide sufficient levels of security at the same time, service providers could implement two factor authentication solutions, which let users choose between knowledge-based and biometric authentication schemes, each combined with an additional token.

4.1 Limitations

The present study suffers from several flaws. First, we used snowball sampling, resulting in a skewed (i.e., younger, higher educated and eventually over-averagely tech-savvy) sample, compared to the general population. Further studies should be based on more heterogeneous samples to allow for generalization. Second, we chose to aim for a brief survey and therefore asked for biometric authentication in general. However, it is possible that different biometric authentication schemes are preferred for different reasons. Hence, it would be valuable to differ between biometric authentication schemes like fingerprint, iris or face recognition in future studies. We also focused on authenticating on a laptop, hence the results might be different when users are asked to evaluate the use of biometric and knowledge-based authentication schemes on their smartphones. Furthermore, it could be interesting to consider a broader range of usage scenarios.

4.2 Conclusion

There seem to be two different user groups, preferring either text passwords or biometric authentication. However, the overall preference can differ from those reported for particular usage scenarios. Important reasons for supporters of both authentication methods are security, efficiency and habit. Furthermore, some users prefer text passwords because they don't require the user to provide personal information. To please all of their users, service providers should offer both authentication methods.

Acknowledgements

This work was supported by the German Federal Ministry of Education and Research (BMBF) within CRISP and MoPPa.

References

Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., & Möller, S. (2011). On the need for different security methods on mobile phones. In *Proceedings of the 13th international conference on human computer interaction with mobile devices and services* (pp. 465–473). MobileHCI '11. Stockholm, Sweden: ACM. doi:10.1145/2037373.2037442

Bhagavatula, C., Ur, B., Iacovino, K., Kywe, S. M., Cranor, L. F., & Savvides, M. (2015). Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption. In *Proceedings 2015 workshop on usable security*. doi:10.14722/usec.2015.23003

Bonneau, J., Bursztein, E., Caron, I., Jackson, R., & Williamson, M. (2015). Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google. In *Proceedings of the 24th international conference on world wide web* (pp. 141–150). doi:10.1145/2736277.2741691

Coventry, L., De Angeli, A., & Johnson, G. (2003). Usability and biometric verification at the atm interface. In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 153–160). CHI '03. Ft. Lauderdale, Florida, USA: ACM. doi:10.1145/642611.642639

Dörflinger, T., Voth, A., Krämer, J., & Fromm, R. (2010). "my smartphone is a safe!" - the user's point of view regarding novel authentication methods and gradual security levels on smartphones. In S. K. Katsikas & P. Samarati (Eds.), *Secrypt* (pp. 155–164). SciTePress.

Furnell, S. & Evangelatos, K. (2007). Public awareness and perceptions of biometrics. *Computer Fraud & Security*, *2007*(1), 8–13. doi:10.1016/S1361-3723(07)70006-4

Inglesant, P. G. & Sasse, M. A. (2010). The true cost of unusable password policies: Password use in the wild. In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 383–392). CHI '10. Atlanta, Georgia, USA: ACM. doi:10.1145/1753326.1753384

Jones, L. A., Antón, A. I., & Earp, J. B. (2007). Towards understanding user perceptions of authentication technologies. In *Proceedings of the 2007 acm workshop on privacy in electronic society* (pp. 91–98). WPES '07. Alexandria, Virginia, USA: ACM. doi:10.1145/1314333.1314352

Leiner, D. J. (2016). SoSci Survey (Version 2.6.00-i). Retrieved from https://www.soscisurvey.de

Mey, G. & Mruck, K. (2010). Grounded-Theory-Methodologie. In G. Mey & K. Mruck (Eds.), *Handbuch qualitative forschung in der psychologie* (pp. 614–626). Wiesbaden: VS Verlag für Sozialwissenschaften. doi:10.1007/978-3-531-92052-8_43

Rodrigues, P. & Santos, H. (2013). Health users' perception of biometric authentication technologies. In *Proceedings of the 26th ieee international symposium on computer-based medical systems* (pp. 320–325). doi:10.1109/CBMS.2013.6627809

Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers & Security*, *61*, 130–141. doi:https://doi.org/10.1016/j.cose.2016.05.007

Stobert, E. & Biddle, R. (2013). Memory retrieval and graphical passwords. In *Proceedings of the ninth symposium on usable privacy and security* (15:1–15:14). SOUPS '13. Newcastle, United Kingdom: ACM. doi:10.1145/2501604.2501619

Tari, F., Ozok, A. A., & Holden, S. H. (2006). A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proceedings of the second symposium on usable privacy and security* (pp. 56–66). SOUPS '06. Pittsburgh, Pennsylvania, USA: ACM. doi:10.1145/1143120.1143128

Toledano, D. T., Fernández Pozo, R., Hernández Trapote, Á., & Hernández Gómez, L. (2006). Usability evaluation of multi-modal biometric verification systems. *Interacting with Computers*, *18*(5), 1101–1122. doi:10.1016/j.intcom.2006.01.004

Wimberly, H. & Liebrock, L. M. (2011). Using Fingerprint Authentication to Reduce System Security: An Empirical Study. In *2011 ieee symposium on security and privacy* (pp. 32–46). IEEE. doi:10.1109/SP.2011.35

Zimmermann, V. & Gerber, N. (in press). „I fit wasn't secure, they would not use it in the movies" - Security Perception and User Acceptance of Authentication Technologies. In *Hci international*.

Autoren

Gerber, Nina

Nina Gerber studierte Psychologie an der Technischen Universität Darmstadt. Seit Anfang 2015 ist sie dort am Institut für Psychologie als wissenschaftliche Mitarbeiterin in der Forschungsgruppe für Arbeits- und Ingenieurpsychologie tätig. Ihre Forschungsinteressen liegen hauptsächlich im Bereich der Mensch-Maschine-Interaktion. In mehreren Kooperationsprojekten mit dem Fachbereich Informatik beschäftigt sie sich aktuell damit, wie Nutzer im Technikkontext mit privatsphäre-kritischen Daten umgehen.

Zimmermann, Verena

Verena Zimmermann finished her studies of Psychology at the Technische Universität Darmstadt in 2015. After a research stay at Griffith University, Brisbane, she started working as a researcher and PhD student in the Department of Psychology back in Darmstadt in the group Work and Engineering Psychology in 2016. Her research interests cover Usable IT Security, Human-Computer-Interaction and Human Factors in Safety and Security.