Universal Design 2024: Shaping a Sustainable, Equitable and Resilient Future for All
K.S. Fuglerud et al. (Eds.)
© 2024 The Authors.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License 4.0 (CC BY-NC 4.0).
doi:10.3233/SHTI241036

Towards Recommendations for the Universal Design of Online Authentication Systems

Helen PETRIE[1, a] and Suzanna SCHMEELK[a, b]
[a] *Department of Computer Science, University of York, York YO10 5GH, UK*
[b] *Department of Computer Science, Mathematics and Science, St John's University, Queens NY 11439, USA*
ORCiD ID: Helen Petrie: orcid.org/0000-0002-0100-9846
Suzanna Schmeelk: orcid.org/0000-0003-1886-3798

Abstract. There is a growing body of research on the problems older and disabled people face with authentication systems and a range of solutions have been developed. However, this research has not been integrated across user groups and solutions usually only target one or two groups. This research has attempted to integrate the empirical research findings across studies conducted with people with visual, physical, and intellectual disabilities, people dyslexia and older people. It proposes an initial set of 15 recommendations for the universal design of authentication systems. Four recommendations are about authentication systems in general, six about password authentication, two about CAPTCHAs and three about biometric authentication. 40% of the recommendations address problems experienced by at least two different user groups and over 25% address problems experienced by three groups. However, much further work is needed to validate and refine the recommendations and integrate them into a universal design approach.

Keywords. People with disabilities, authentication, universal design, recommendations

1. Introduction

As more and more services move online, the number of online accounts we are all are required to use continues to grow. Often the information stored in these accounts is personal and valuable to us, be it financial information or personal photos, so ensuring the information is secure is vitally important. Therefore, we need to authentication ourselves when logging into online accounts and take appropriate measures to make sure our accounts and data are secure.

There are now numerous forms of authentication, including:

- Passwords, which often include complex requirements (e.g. the password must be 8 characters long and contain at least one capital letter, one number and one special character from a specified set) and password strength meters to inform users whether their proposed password is sufficiently strong;

[1] Corresponding Author: Helen Petrie, helen.petrie@york.ac.uk

- CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart), which can involve reading distorted letters, finding all the examples of a particular object in a set of phones (e.g. click on all the photos with a car in them), or solving a puzzle;
- two factor and multi-factor authentication, in which the user must enter more than one form of identification, often including a one-time code, for example I enter a password into an account login and the account then sends me a code on a different device I have registered, such as my smartphone, I must then enter this code before I get access to the account;
- biometric authentication, which may be via fingerprint, face, voice or iris recognition.

Some of these authentication methods are difficult even for young, able-bodied people to use and people with disabilities and older people face many additional difficulties, as well as anyone with a situational disability, for example a broken arm, a slow internet connection or a very small screen. Inevitably, as in other technological areas, these methods are only designed with able-bodied, computer literate users in mind, inclusive options are very much an afterthought and are often less than optimal. However, there is now a growing body of research about the problems encountered by older and disabled people with authentication systems and a range of solutions to these problems, usually proposed to support one specific user group. The research in these two areas is outlined briefly in the next section.

The main purpose of our research is to review the evidence on the problems that older and disabled people encounter with authentication and to propose recommendations to support the universal design of authentication systems. The motivation for the work is twofold. Firstly, the evidence of the problems older and disabled people encounter is dispersed through many research papers and needs to be drawn together. Not only is this corpus of research of interest in itself, but one of the interesting aspects of the research is that while people with very different disabilities have different problems, the solutions we can offer can often address more than one group. This is an important observation which does not seem to have been made about the body of research. In our previous work, we found this economy of solutions was often the case in web accessibility problems [10]. Secondly, this is a very important observation to communicate to developers of systems, who we have found are often overwhelmed by the prospect of meeting the needs of people with many different disabilities. But the task facing them is not as daunting as they may think, and sophisticated implementations can often solve numerous accessibility problems. Nonetheless, the set of recommendations presented here are only a preliminary version, which require further research and validation, plans for which will be discussed briefly at the end of the paper.

2. Background

In this section we concentrate on research which has directly engaged with older and disabled people. We have not yet documented our literature search as a systematic review, however, we have been collecting literature on this topic for some time, and augmented our collection with searches in the ACM and IEEE Xplore digital libraries and Google Scholar for papers with a wide range of keywords. We will continue to expand our search

into a systematic review, appropriately documented. A number of papers have addressed the issues of the accessibility of authentication systems from a theoretical perspective, analysing systems using what is known about the characteristics of the different user groups [3, 20, 29]. While useful, this research may miss the actual lived experience of older and disabled people and the problems they encounter. Instead, we reviewed research which has used focus groups, questionnaires, interviews and contextual inquiry to directly ask people about the issues they face in order to provide an empirical basis for the recommendations.

Research documenting the problems encountered by older and disabled people has been strongly focused on the problems encountered by visually disabled people (particularly people using screen readers). Research has highlighted a range of problems including the inaccessibility of visual CAPTCHAs [21, 39] and other authentication components which are visual [21, 39], systems which time-out too quickly for screen reader users [21, 39], an inability to determine whether the authentication has been successful [11], and concerns about "shoulder surfing" (either visually or auditorily) [2, 12]. Recent research [34, 40] has shown that although auditory CAPTCHAs are now common, they are not widely available and even when they are, often still create problems for visually disabled users.

There is much less research which has engaged with other disabled user groups. Several studies with people with dyslexia [23, 36] have found that they have difficulties creating and using passwords, due to the need for precise ordering of elements; problems with CAPTCHAs, particularly if they involve reproducing distorted letters and other authentication systems which require pattern recognition. Several studies with people with a range of intellectual disabilities [19, 27] found that people had difficulties creating and using passwords, but also frustration that systems did not provide more specific error messages (e.g. whether it is a username or password which is incorrect). One study with people with upper limb disabilities [26] identified problems with both passwords (e.g. long, complex passwords can be difficult to enter) and biometric authentication, for example the need to remain still, the need to position oneself correctly in relation to the camera or sensor. Only one paper could be found which engaged with people with hearing disabilities [9] but no specific information about the problems they faced was reported. Finally, several papers [8, 33] with older people found that they had problems understanding the requirements, creating and remembering strong passwords (although many solved this problem by writing them down in a secure place).

Research on solutions to authentication problems has also been mainly concentrated on blind people. The most important development has been that of auditory CAPTCHAs [e.g. 22], which are the only alternative authentication mechanism to be widely adopted. However, implementations are not without their own accessibility problems [34, 40]. Other alternatives have been proposed for visually disabled people using tactile authentication [4, 5, 13, 24, 44] and an audio one-time password system [15]. The latter could also be helpful to older people, people with intellectual disabilities and dyslexia. A password manager accessible to visually disabled people has also been proposed [6].

A number of solutions have also been proposed to make authentication easier for older people. These include using graphical passwords to reduce the cognitive load of remembering passwords and adapting them with age-appropriate materials (e.g. older faces) to improve performance. Solutions have also been proposed involving users own doodles, handwriting [37] and musical motifs [17, 28]. Graphical passwords have also been proposed for people with dyslexia [12]. Finally, several solutions have been

proposed to help people with physical disabilities including brain-computer interfaces [38] and a system based on recognition of cardiac rhythms [25].

3. Towards recommendation for universal design of online authentication systems

Table 1: Initial recommendations for a universal design approach to online authentication

Recommendation	Groups supported	Source/s of evidence
GENERAL		
Make the flow in complex authentication tasks clear and explained, logical in a screen reader	Visually disabled people People with dyslexia Older people	[34] [23] [33]
Make it very easy to increase time limits in authentication process	Visually disabled people Older people People with dyslexia	[21, 39] [33, 42] [12, 23]
Ensure all elements of the system are accessible and identifiable to screen readers (e.g. edit fields, error messages, feedback that authentication is successful)	Visually disabled people	[11, 34, 40]
Mitigate against auditory "shoulder surfing" for screen reader users	Visually disabled people	[11, 45]
PASSWORDS		
Support people in creating strong, secure passwords based on familiar concepts	Older people People with dyslexia	[8, 37] [12, 36]
Make password construction requirements ("policies") clearer	Visually disabled people Older people People with dyslexia	[18, 43] [33] [12, 32]
Provide alternatives to character-based passwords	Visually disabled people People with intellectual disabilities People with upper limb disabilities	[6, 14, 19] [27] [24]
In graphical password systems, allow use of age appropriate elements	Older people	[30, 31]
Provide better support for creating passwords which meet requirements	Older people	[33]
Provide better education on strong passwords and how to create them	Older people	[33]
CAPTCHAs		
Offer alternatives in CAPTCHAs	Visually disabled people People with dyslexia	[21, 39] [23, 32]
If using audio, make sure the source is clear	People with visual disabilities	[34, 40]
BIOMETRIC AUTHENTICATION		
For biometric authentication, ensure that there is auditory/tactile information about where to place finger/face	People with visual disabilities	[7, 11, 16, 35]
Provide alternatives to iris recognition for people without eyes or who cannot open their eyes	People with visual disabilities	[34, 40]
Provide alternatives in biometric authentication which requires the user to be still for a period (e.g. at registration)	People with motor disabilities	[16, 21]

Table 1 summarizes the initial version of the proposed recommendations for the universal design of online authentication systems. It comprises 15 recommendations, four recommendations are about authentication systems in general, six about password authentication, two about CAPTCHAs and three about biometric authentication. The

user groups addressed comprise people with visual, physical and intellectual disabilities, people with dyslexia and older people. 40% (6/15) of the recommendations address problems experienced by two or more different user groups and over 25% (4/15) of the recommendations address problems experienced by three different user groups.

Some of the recommendations might easily apply to other user groups. For example, the recommendation about password authentication in relation to older people, "Support people in creating strong, secure passwords based on familiar concepts" could also support people with intellectual disabilities, but as we did not find empirical evidence for that problem with that user group, thus for the moment we have refrained from including it. Another recommendation in relation to older people, that "In graphical password systems, allow use of age-appropriate elements" is based on research with older people using older and younger faces [30, 31]. It could well be that people with intellectual disabilities would find elements from categories they are familiar with also beneficial, that would be an interesting possibility to research. Finally, these recommendations could be extended beyond the needs of older and disabled people to include other diverse user groups, such as users of different ethnicities and cultures (so for example, culturally and ethnically appropriate elements would a useful extension of the recommendation of "age-appropriate elements" to "age-appropriate and culturally and ethnically appropriate elements"). Finally, examples provided with the recommendations could include those involving situational disabilities, to illustrate the broad application of their use.

Some of the recommendations can also benefit from further elaboration and examples. An example is "Make it very easy to increase time limits in authentication process". Visually disabled screen reader users in attempting to use auditory CAPTCHAs can find that there is not sufficient time allowed between listing to the auditory message and navigating to the field in which the answer needs to be entered, causing them to be timed out. Thus, it is not just the overall time limits that are important, but the time limits on individual steps in the authentication journey. Another example, again for visually disabled screen reader users, is "If using audio make sure the source is clear". Of course, developers do not have control over the environment in which an audio CAPTCHA is used, so this does not refer to noise in the environment. However, there may be a temptation to distort the audio source in analogy to the distortion of a visual CAPTCHA or to use naturally captured audio material which may not be clear (Google appear to have done this), but combined with uncontrollable environmental conditions, these manipulations would adversely affect the effectiveness of the audio CAPTCHA.

4. Conclusions

In this paper we have presented an initial set of recommendations for the universal design of authentication systems, covering the needs of older people and a range of people with different disabilities. However, much further work is needed to validate and refine these recommendations. Some of the empirical research on which the recommendations are based is now over a decade old, and authentication systems have evolved considerably since then. It is notable that none of the recommendations deal explicitly with two or multi factor authentication, although these types of authentication are now widely used. In addition, none of the recommendations deal with single sign-on or federated identity management systems, also now widely used. We have not found any empirical research with older or disabled users in those areas yet. In addition, some of the research

understandably is based on very small samples of participants, so may not be typical of the whole user group, particularly as these user groups are very diverse in themselves. Thus, our future work will be to valid and refine the recommendations by further research with the user groups to establish how representative and severe the problems underlying the recommendations are, both using questionnaires and testing of simulations of authentication systems exhibiting the problems. The recommendations also need to be scrutinized for any aspects which would involve compromising the security of the authentication, as this would defeat their purpose. Other research could investigate extensions of specific recommendations to other user groups for which we did not find any empirical evidence. Finally, this research has taken an essentially bottom-up process, looking for the empirical evidence from users of the problems they have. It will now be interesting to combine this with a top-down approach, starting from the basic principles of universal design and applying these to what we have learnt about the problems encountered.

A general principle which emerges from the review of research and the recommendations is the need for flexibility and personalization in authentication systems. In researching this paper, we encountered a very interesting example of a proposal for a multimodal authentication system [1], which would incorporate visual, verbal and spatial cues (and could easily be extended to incorporate auditory cues). Although this system was not targeted at older or disabled users, an implementation of such an authentication system developed using some of the recommendations could be an excellent exemplar of a universally designed authentication system.

References

[1] Al-Ameen, M.N., Wright, M., & Scielzo, S. (2015). Towards making random passwords memorable: Leveraging users' cognitive ability through multiple cues. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI 15). ACM Press.

[2] Ahmed, T., Hoyle, R., Connelly, K., Crandall D., and Kapadia, A. (2015). Privacy concerns and behaviors of people with visual impairments. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. (CHI 15). ACM Press.

[3] Andrew, S., Watson, S., Oh, T., & Tigwell, G. W. (2020). A review of literature on accessibility and authentication techniques. Proceedings of the 22nd International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS 22). ACM Press.

[4] Azenkot, S., Rector, K., Ladner, R., & Wobbrock, J. (2012). PassChords: secure multi-touch authentication for blind people. Proceedings of the 14th international ACM SIGACCESS conference on Computers and accessibility (ASSETS 12). ACM Press.

[5] Balaji, V., Kuppusamy, K.S., & Afzal, S. (2017). VIBI: A Braille inspired password entry model to assist person with visual impairments. Smart Secure Systems – IoT and Analytics Perspective: Proceedings of the International Conference on Intelligent Information Technologies (ICIIT 2017). Springer.

[6] Barbosa, N.M., Hayes, J. & Wang, Y. (2016). UniPass: design and evaluation of a smart device-based password manager for visually impaired users. Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '16). ACM Press.

[7] Blanco-Gonzalo, R., Lunerti C., Sanchez-Reillo, R., & Guest, R.M. (2018) Biometrics: accessibility challenge or opportunity? PLoS ONE 13(3): e0194111. https://doi.org/10.1371/journal.pone.0194111

[8] Carter, N. C. (2015). Graphical passwords for older computer users. Adjunct Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology (UIST '15 Adjunct). ACM Press.

[9] Correia, W., Penha, M. Macedo, J. et al. (2019). Full mobile accessibility is a matter of respect: GuAMA update process for motor and hearing disability users. Proceedings of the 18th Brazilian Symposium on Human Factors in Computing Systems (IHC '19). ACM Press.

[10] Disability Rights Commission. (2004). The web: access and inclusion for disabled people. A formal investigation by the Disability Rights Commission. London: The Stationery Office.

[11] Dosono, B., Hayes, J. & Wang. Y. (2015). "I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication. Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS 2015). USENIX.
[12] Evtimova, P., & Nicholson, J. (2021). Exploring the acceptability of graphical passwords for people with dyslexia. Proceedings of INTERACT 2021: Lecture Notes in Computer Science 12932. Springer.
[13] Faustino, D. B., & Girouard, A. (2018a). Bend passwords on BendyPass: A user authentication method for people with vision impairment. Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS 20). ACM Press.
[14] Faustino, D. B., & Girouard, A. (2018b). Understanding authentication method use on mobile devices by people with vision impairment. Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS 20). ACM Press.
[15] Fuglerud, K. & Dale, O. (2011). Secure and inclusive authentication with a talking mobile one-time-password client. IEEE Security & Privacy, 9(2), 27-34.
[16] Furnell, S., Helkala, K., & Woods, N. (2021). Disadvantaged by disability: Examining the accessibility of cyber Sscurity. In M. Antona & C. Stephanidis (Eds.), Universal Access in Human-Computer Interaction. Design Methods and User Experience (Proceedings of HCII 2021). Springer.
[17] Gibson, M., Renaud, K., Conrad, M. & Maple, C. (2015). Play that funky password!: Recent advances in authentication with music. In M. Gupta (Ed.), Handbook of Research on Emerging Developments in Data Privacy. IGI Global.
[18] Hayes, J., Dosono, B., & Wang, Y. (2017). "They should be convenient and strong": Password perceptions and practices of visually impaired users. Proceedings of iConference 2017 Proceedings. iSchools.
[19] Hayes, J., Li, X. & Wang, Y. (2017). "I Always Have to Think About It First": authentication experiences of people with cognitive impairments. Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS 17). ACM Press.
[20] Helkala, K. (2012). Disabilities and authentication methods: usability and security. Proceedings of the 7th International Conference on Availability, Reliability and Security. IEEE.
[21] Holman, J., Lazar, J., & Feng, J. (2008). Investigating the security-related challenges of blind users on the web. In Langdon, P., Clarkson, J., Robinson, P. (Eds.), Designing Inclusive Futures. Springer.
[22] Holman, J., Lazar, J., Feng, J.H., & D'Arcy, J. (2007). Developing usable CAPTCHAs for blind users. Proceedings of the 9th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '07). ACM Press.
[23] Kelly, N. & Petrie, H. (2022). Digital Authentication and Dyslexia: A Survey of the Problems and Needs of Dyslexia People. In Miesenberger, K., Kouroupetroglou, G., Mavrou, K., Manduchi, R., Covarrubias Rodriguez, M., & Penáz, P. (Eds.), Computers Helping People with Special Needs. ICCHP-AAATE 2022. Lecture Notes in Computer Science, vol 13342. Springer.
[24] Kuber, R., & Sharma, S. (2010). Toward tactile authentication for blind users. Proceedings of the 12th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '10). ACM Press.
[25] Lewis, B., Hebert, J., Venkatasubramanian, K., Provost, M., & Charlebois, K. (2020). A new authentication approach for people with upper extremity impairment. 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE.
[26] Lewis, B., & Venkatasubramanian, K. (2021). "I … Got my Nose-Print. But it Wasn't Accurate": How people with upper extremity impairment authenticate on their personal computing devices. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI 2021). ACM Press.
[27] Ma, Y., Feng, J., Kumin, L. & Lazar, J. (2013). Investigating user behavior for authentication methods: A comparison between individuals with Down syndrome and neurotypical users. ACM Transactions on Accessible Computing, 4(4).
[28] Marne, S.T., Al-Ameen, M.N., & Wright, M.K. (2017). Learning system-assigned passwords: a preliminary study on the people with learning disabilities. Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS 2017), USENIX Association.
[29] Moreno, L., González, M. & Martınez, P. (2014). CAPTCHA and accessibility - Is this the best we can do? Proceedings of the 10th International Conference on Web Information Systems and Technologies - Volume 1: WEBIST.
[30] Nicholson, J., Coventry, L. & Briggs, P. (2013). Age-related performance issues for PIN and face-based authentication systems. Proceedings of the 2013 SIGCHI Conference on Human Factors in Computing Systems (CHI 13). ACM Press.
[31] Nicholson, J., Coventry, L. & Briggs, P. (2013). Faces and pictures: understanding age differences in two types of graphical authentications. International Journal of Human-Computer Studies, 71(10), 958-966.

[32] Ophoff, J., Johnson, G. & Renaud, K. (2021). Cognitive function vs. accessible authentication: insights from dyslexia research. Proceedings of the 18th International Web for All Conference (W4A 18). ACM Press.
[33] Petrie, H., Merdenyan, B., and Xie, C. (2022). Password Challenges for Older People in China and the United Kingdom. In Miesenberger, K., Kouroupetroglou, G., Mavrou, K., Manduchi, R., Covarrubias Rodriguez, M., & Penáz, P. (Eds.), Computers Helping People with Special Needs. ICCHP-AAATE 2022. Lecture Notes in Computer Science, vol 13342. Springer.
[34] Petrie, H., Moreno, L. & Schmeelk, S. (2023). Accessibility barriers with authentication methods for blind and partially sighted people in the Spanish-speaking world. Proceedings of the British Computer Society Human Computer Interaction Conference 2023. BCS. DOI: 10.14236/ewic/BCSHCI2023.22
[35] Petrie, H. & Wakefield, M. (2020). Remote moderated and unmoderated evaluation by users with visual disabilities of an online registration and authentication system for health services. Proceedings of the 9th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion (DSAI 2020). ACM Press.
[36] Renaud, K., Johnson, G., & Ophoff, J. (2021). Accessible authentication: dyslexia and password strategies. Information and Computer Security, 29(4), 604 – 624.
[37] Renaud, K. & Ramsay, J. (2007). Now what was that password again? a more flexible way of identifying and authenticating our seniors. Behaviour and Information Technology 26(4), 09-322.
[38] Saulynas, S., & Kuber, R. (2017). Towards brain-computer interface (BCI) and gestural-based authentication for individuals who are blind. Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS 17). ACM Press.
[39] Sauer, G. Holman, J., Lazar, J., Hochheiser, H. & Feng, J. (2010). Accessible privacy and security: a universally usable human-interaction proof tool. Universal Access in the Information Society, 9, 239 – 248.
[40] Schmeelk, S. & Petrie, H. (2022). Digital Authentication for Visually Disabled People: Initial Results of an Online Survey In Miesenberger, K., Kouroupetroglou, G., Mavrou, K., Manduchi, R., Covarrubias Rodriguez, M., & Penáz, P. (Eds.), Computers Helping People with Special Needs. ICCHP-AAATE 2022. Lecture Notes in Computer Science, vol 13342. Springer.
[41] Shih, M.-S., Chang, J.-H., & Cheng, T.-Y. (2019). The design guideline for dyslexics-friendly Chinese ATM interface. Proceedings of the 10th International Conference on E-Education, E-Business, E-Management and E-Learning, Tokyo, Japan. https://doi.org/10.1145/3306500.3306519
[42] Sreeramareddy, L., Mulbah, P. and Feng, J.H. (2015). Investigating the use of gesture-based passwords by the seniors. In T. Tryfonas and I. Askoxylakis, (Eds.), Human Aspects of Information Security, Privacy, and Trust (HAS 2015). Lecture Notes in Computer Science, vol 9190. Springer, Cham.
[43] Vu, KP.L. & Hills, M.M. (2013). The influence of password restrictions and mnemonics on the memory for passwords of older adults. In Yamamoto, S. (Ed.), Human Interface and the Management of Information: Information and Interaction Design. Lecture Notes in Computer Science, vol 8016. Springer.
[44] Wolf, F., Kuber, R., & Aviv, A. J. (2017). Perceptions of mobile device authentication mechanisms by individuals who are blind. Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS 17). ACM Press.
Zhu, S., Ma, Y., Feng, J., & Sears, A. (2009). Don't listen! I am dictating my password! Proceedings of the 11th international ACM SIGACCESS conference on Computers and accessibility (ASSETS '09). ACM Press.