Cognitive function vs. accessible authentication: insights from dyslexia research

Jacques Ophoff
Graham Johnson
Karen Renaud

Cognitive Function vs. Accessible Authentication: Insights from Dyslexia Research

Jacques Ophoff, Graham Johnson
{j.ophoff,g.johnson}@abertay.ac.uk
Abertay University
Dundee, United Kingdom

Karen Renaud
karen.renaud@strath.ac.uk
University of Strathclyde
Glasgow, United Kingdom

ABSTRACT

The most common authentication mechanism, the password, requires a user to recall a secret. Users take this memorisation, or cognitive function, test on a daily basis in order to gain access to systems and devices. This mechanism's design has received much scrutiny and there is a common realization that security and usability are key considerations. In this paper, we consider a third, emergent aspect: that of *accessibility*. Using a qualitative approach, we explore the challenges current password-based approaches pose to people with dyslexia, a relatively common cognitive disability, highlighting several issues. Following draft web accessibility guidelines, we also evaluate alternative authentication mechanisms. We observe a lack of consideration for accessibility in the area of authentication and offer suggestions for future research.

CCS CONCEPTS

• **Human-centered computing** → **Accessibility**; *Accessibility design and evaluation methods*; *Accessibility systems and tools*; • **Security and privacy** → **Authentication**; *Usability in security and privacy*; • **Social and professional topics** → **People with disabilities**.

KEYWORDS

Cognitive Function, Accessibility, Authentication, Passwords, Dyslexia

ACM Reference Format:
Jacques Ophoff, Graham Johnson and Karen Renaud. 2021. Cognitive Function vs. Accessible Authentication: Insights from Dyslexia Research. In *Proceedings of the 18th International Web for All Conference (W4A '21), April 19–20, 2021, Ljubljana, Slovenia.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3430263.3452427

1 INTRODUCTION

Authentication is a fundamental part of every system where access control needs to be enforced. People have become accustomed to frequent demands to authenticate themselves, often on a daily basis. This usually requires the recall of a password, which can also be regarded as a 'cognitive function test'. To ensure the reliable and resilient operation of systems, software engineers take great care to design and implement such authentication mechanisms securely. Usability is often a secondary consideration [1], although it has received more attention, deservedly, over the last two decades [15].

While there has been a great deal of focus on the correct technical implementation and usability of authentication mechanisms, the same cannot be said for accessibility. Accessibility guidelines, such as the Web Content Accessibility Guidelines (WCAG) published by the Web Accessibility Initiative (WAI) of the W3C, does not currently make any substantive reference to authentication. Arguably, this should be considered an additional dimension to be acknowledged and deliberated above and beyond the longstanding debate on security and usability tensions.

In this paper, we examine accessible authentication from the perspective of those with dyslexia, drawing on their real-world experiences of routine authentication. Our previous work provides a comprehensive review of extant research into the impact of dyslexia on password usage, discovering a relative neglect of this field [13]. Subsequently we explored the difficulties people with dyslexia face, their general experiences with passwords, the coping strategies they use, and the advice they can provide to developers and others who struggle with passwords [14]. Here we focus specifically on the WCAG and alternative authentication mechanisms which could enhance accessibility. We recruited 13 participants with dyslexia and conducted in-depth online semi-structured interviews to learn about their varied experiences and challenges, and to understand their coping strategies. Using these insights, derived from our field data, this paper considers the ways in which accessibility standards could be informed by user-centred research, in order to provide an inclusive user experience which accommodates those with dyslexia and related difficulties.

This paper is structured as follows. In Section 2, we examine related work on authentication and cognitive function tests, after which we explore some of the key issues revealed by our interview data and analysis. In Section 3, we evaluate draft WCAG requirements on alternative (authentication and verification) mechanisms and explore possible trade-offs that should be considered by system designers, developers, and operators. Finally, Section 4 concludes with recommendations for future work.

2 AUTHENTICATION AND COGNITIVE FUNCTION TESTS

Authentication is the act of "verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system" [4]. This is usually accomplished using one of three factors: 'something you know', such as a password (knowledge); 'something you have', such as an access card (possession); or 'something you are', such as a fingerprint (inherence). It

W4A '21, April 19–20, 2021, Ljubljana, Slovenia

ACM ISBN 978-1-4503-8212-0/21/04…$15.00
https://doi.org/10.1145/3430263.3452427

is possible to provide additional layers of protection by combining two or more factors, also known as multi-factor authentication.

Of these factors, knowledge of a secret password is by far the most commonly deployed, mainly due to the ease of implementation and familiarity to users. The use of passwords relies on a type of cognitive function test, that can be described as "a task that requires the user to remember, manipulate, or transcribe information" [20]. Such tests are known to be especially problematic for users with cognitive disabilities with difficulties extending beyond passwords to things such as remembering patterns, PINs, tokens, and identifying objects within images (CAPTCHAs). Previous research has explored the effect of cognitive load and memory limitations on password choices [7, 12].

A significant proportion of the world's population experiences some degree of dyslexia, which can have a major impact when they need to authenticate themselves via cognitive function tests. Dyslexics can be either 'dysphonetic' or 'dyseidetic' [5]. Someone with dysphonetic dyslexia has difficulty connecting sounds to symbols, so might struggle to sound out words, and is likely to make spelling mistakes. The dyseidetic individual, while having a good grasp of phonetic concepts, experiences difficulty recognising whole words and also struggles with spelling. Passwords are supposed to be 'nonwords' so, according to Newby [11], dysphonetic dyslexics will struggle to spell words they are unfamiliar with, which will challenge their ability to break down passwords into characters to re-enter them. Dyseidetic dyslexics, on the other hand, will have "exceptional difficulty with nonphonetic words" [5, p.122], and spelling them.

Passwords are supposed to be nonwords, which means that both types of dyslexics will struggle to break a password down into individual letters correctly due to their spelling difficulties. Dyseidetic dyslexics will struggle to memorise their passwords because they cannot rely on their visual memory to memorise an obfuscated password. Dysphonetic dyslexics are likely to be challenged by the need to decipher and implement complex password requirements (upper case, lower case etc.) due to their impaired ability to recognise words.

The need for a deeper understanding of the accessibility of authentication mechanisms has been acknowledged for specific cognitive disabilities, such as Down syndrome [10], as well as cognitive impairments more generally [2, 8]. Following a comprehensive review of the literature, we discovered a lack of knowledge on the experiences people with cognitive disabilities (in our case dyslexia) have with passwords, and what that might imply for cognitive function tests [13]. Therefore, we decided to explore this topic systematically using a qualitative field research approach [24], one which entailed a semi-structured conversational and empathic approach [14]. Given the SARS-Cov-2 situation, these interviews were conducted remotely via contemporary video meeting tools.

2.1 Problematic Issues

We asked the participants about their views on the most difficult elements of password usage which can be considered as a type of cognitive function test. Several significant issues were highlighted across a range of different elements and scenarios. Problems were experienced in the creation, use, and the management of passwords. Many of the participants found it problematic to satisfy the complexity requirements which are commonly enforced in order to ensure stronger passwords. They struggled to meet the requirements, and also to remember the resulting, changed password:

> "*But if then I'm asked to add exclamation marks, figure shapes or stars [special characters], that's a troublesome one. Especially when, once you've done it, they say this is not secure enough!*" (Participant 11)

The repetition of a password, used to ensure the user has typed what they intended to, and to help them remember it, also presented them with significant challenges: *"I spell them incorrectly. Especially if you have to type the password and confirm it. I can't do it the same twice."* (Participant 5). Remembering passwords was a common difficulty for our study participants. Participant 12 explained:

> "*Somebody else might be able to go, you know, right it was cat spelt with an 'a' or it was alpha spelled with a '@' sign. My brain doesn't seem to remember that. And then occasionally I'll reverse things or reverse letters and I won't notice it and then I put the same thing again and again, and then suddenly it works…*"

This was often exacerbated by fatigue or frustration. As a consequence, account lockout (due to exceeding the limit of incorrect attempts) occurred frequently and sometimes required the person to create a new account altogether: *"…it takes up a lot of my time re-registering for things, and password recovery, so much time…"* (Participant 8).

Several participants managed passwords by physically writing them down. An interesting approach was saving passcodes or PINs as Smartphone address book entries:

> " *…I put these numbers in my phone. So I pretend it's a person and I make up a phone number, and the last four digits of that phone number are the PIN number."* (Participant 10)

Using a password manager was suggested as a possible solution, yet most participants still preferred remembering individual passwords:

> "*But I also try to remember it in case LastPass [a well-known password manager] goes wrong; then I can still remember my passwords to the apps."* (Participant 3)

The use of numbers, such as PINs, also presented problems. This form of authentication is frequently used, either as a primary or secondary factor to secure transactions. Participant 7 related that:

> "*Any time I have to enter a number, even a few digits, that's really tricky. When I have to enter numbers online I get my husband to check it. I check things about three times to make sure it is right."*

The length of time available to process a number also introduced frustration: *"My biggest one is my banking. It creates a completely unique number every time I want to log in. So, I use this little press pad, and this little screen comes up with a number – my brain won't remember that number, and it doesn't stay up long enough for me to get it into my computer."* (Participant 8).

Participants also mentioned difficulties using CAPTCHAs when a font is distorted as part of the test: *"If you want me to tell you what the most difficult thing and the most frustrating thing is -– the wiggly*

capture codes you have to put in on the computer…" (Participant 11). This problem was not necessarily present when the test was in a graphical form, e.g. select all the pictures with traffic lights. However, a common workaround in both cases was switching to the audio option:

> "*I don't mind the ones where you have to click all the crosswalks, or click all the traffic lights, but if it's one of the ones that's got capitals and numbers for squiggly lines, I can't see it. I always just change it to audio so it speaks at me.…*" (Participant 8)

In summary, our data suggests that people with dyslexia, with all of its cognitive implications, can experience a range of challenges when encountering, in essence, a cognitive function test. This extends beyond passwords to the use of sequences of numbers, and to some kinds of CAPTCHAs. Our data complements previous research [8], which included one participant with dyslexia, with a more detailed description of authentication experiences. It should also be noted that difficulties occur not only when trying to remember the secret information, but across the whole life cycle of creation, use, refresh, and management of passwords, as noted by the Cognitive and Learning Disabilities Accessibility Task Force (Coga TF) [17] in their use of scenarios.

The work of the Coga TF [19] is a combined effort of the Web Content Accessibility Guidelines Working Group (AG WG) and the Accessible Platform Architectures (APA) Working Group addressing understanding and guidance with respect to cognitive issues. The Task Force has produced clear guidance on site design and user needs where this relates to people with learning and cognitive difficulties. Their gap analysis [18] clearly identifies some of the issues with web security and privacy technologies, and potential solutions. The cognitive issues, access challenges (especially with regard to creation, memory of and management of passwords) and alternatives align with findings from our primary research driven by people with dyslexia. From a research perspective, the W3C Cognitive Accessibility User Research [22] focuses on many learning or cognitive disabilities, including dyslexia (but also aphasia, dyscalculia, autism etc.), and is driving the development of strategies to improve accessibility across specified groups.

2.2 WCAG Requirements

WCAG 2.1, which was published as a W3C Recommendation in June 2018, does not contain any substantive reference to authentication. However, this gap may be addressed, hopefully, in the next version of the guidelines (WCAG 2.2), which is currently available as a Working Draft published in August 2020 [21]. WCAG 2.2 introduces a new success criterion called 'Accessible Authentication' (3.3.7) which requires that:

> For each step in an authentication process that relies on a cognitive function test, at least one other method is available that does not rely on a cognitive function test [20].

This will allow users to authenticate, regardless of the level of their cognitive abilities. Examples of other methods could be a password manager automatically filling in credentials, using a device (e.g., with biometrics), or using a third-party login provider.

Currently five 'sufficient mechanisms' are proposed as alternatives by the WCAG Working Group. Of these mechanisms only one — Email link authentication — is described in detail. This mechanism should provide a link that can be emailed to the user and, upon clicking the link, they are redirected to the website and automatically logged in. This method, also known as 'magic links', is convenient but may result in longer processing times and initial feelings of anxiety [23]. The flip side is that security advice often advises users not to open links in emails. The fact that this improvement in accessibility arguably weakens the integrity of the mechanism is something that has to be acknowledged and addressed.

Numerous alternative authentication mechanisms exist which could satisfy the WCAG Accessible Authentication requirement. The next section evaluates some of these mechanisms, specifically looking at suitability for users with dyslexia.

3 EVALUATION OF ALTERNATIVE AUTHENTICATION MECHANISMS

While alphanumeric passwords are the most common knowledge-based authentication factor, numerous alternatives exist. Systematic literature reviews of authentication mechanisms [3, 16] identified at least six '*what you know*', four '*what you hold*', and 15 different '*what you are*' factors (inherence) [16]. Additional considerations for each mechanism are cost and ease of implementation [3]. Ignoring alphanumeric passwords, the ten schemes receiving the most attention from researchers, as represented by research papers, are listed in Table 1.

It is likely that the research interest (number of articles) is to an extent a reflection of availability and convenience, as well as the dominant approaches within everyday systems and services. Several of these mechanisms may be suitable to promote accessibility:

What you know: graphical passwords (but not cognitive authentication) offer a cost-effective and easy to implement mechanism. However, memorisation is still required.

What you hold: smart cards and OTPs (often in combination with a mobile app) have additional costs when hardware-based tokens are involved. However, the mechanism is well understood and easy to implement.

What you are: various biometric mechanisms or hand gestures can range in cost, depending on the complexity of hardware involved. A reliable implementation and reliance on ubiquitous biometric readers may be harder for some mechanisms.

The most common criteria for comparing mechanisms are usability, security and cost [16]. Furthermore, the WCAG adds the criterion of accessibility, which is not commonly considered in authentication literature and is thus an area in need of further research. We provide some initial comments based on our research data.

There was a degree of interest, although very little experience of, graphical, pictorial, and audio/musical 'password' approaches, by our interviewees. Graphical passwords ask the user to recall selected images from a set. While this mechanism is based on a principle of recall there is evidence that memorability is improved, particularly when used with cues, compared to alphanumeric passwords [9]. We found that participants were generally positive about the potential of this approach and perceived this to be more memorable for a

Table 1: Alternative Authentication Mechanisms [3, 16]

No. of Articles	Mechanism	Factor	Cost-Effectiveness	Implementation
103	ID-based (Smart Cards)	What you hold	M	E
43	One Time Password (OTP) tokens	What you hold	L	E
42	Graphical passwords	What you know	L	E
25	Cognitive authentication	What you know	L,M	E
24	Face biometrics	What you are	M,H	H
24	Keystroke biometrics	What you are	L,M	E
21	Mobile-based	What you hold	L,M,H	E
12	Hand gestures	What you are	M,H	H
12	Palmprint biometrics	What you are	M	H
11	Touchstroke biometrics	What you are	L,M	E

Cost-Effectiveness (L indicates Low, M indicates Medium, H indicates High) and Implementation (E indicates Easy, H indicates Hard)

dyslexic: *"That's quite ingenious. I usually remember small details and then I can remember things"* (Participant 3).

A potentially similar mechanism is the use of musical passwords [6]. Based on interview responses, we perceive musical recall to be much easier for dyslexics:

> "*For low risk systems that sounds great. Interestingly enough, music is one Of those things that sticks quite easily.*" (Participant 6)

> "*That would be really interesting. I do tend to remember a tune a lot easier than, you know, a random string of letters.*" (Participant 12)

Smart card-based authentication is the most researched mechanism, particularly in the context of multi-factor authentication [16]. Participants seemed ambivalent about this mechanism (including OTPs, token-based and physical key fobs). We noted that the use of numeric OTPs introduce difficulties, as people struggle to retype numbers correctly (refer Section 2.1) and often need to rely on strategies like reading it aloud to themselves or writing it down. Such strategies may introduce vulnerabilities (e.g. shoulder surfing) and reduce the security of the mechanism. A feature which can assist in this regard is automatic number entry, such as a Smartphone recognising an OTP in a text message:

> "*Luckily modern phones have the ability to automatically input it from the received text. So I almost consistently use that.*" (Participant 13)

Inherence-based mechanisms (what you are) present a range of possibilities, though these frequently require additional hardware and can be more difficult to implement. For the end-user, these mechanisms are convenient — especially fingerprint and face biometrics, which are widely known due to their use in Smartphones. On the area of biometrics some of our respondents were very positive:

> "*So, I've now started using facial recognition on this computer…I don't know whether it's my age and my technophobia. I was a bit concerned to start with, but it's worked absolutely beautifully every single time.*" (Participant 9)

However, we may also note that those verification and authentication mechanisms relying upon biometrics can raise questions of inclusion. There were participants who were concerned (rightly or not) about such mechanisms:

> "*I think that biometric devices, like taking fingerprints and things like that, I have always viewed them as very compromising in terms of security. It seems very suspicious to me that any company should possess copies of your fingerprints.*" (Participant 13)

The variety of attitudes and behaviours with the listed mechanisms suggest that there is no single or 'most appropriate' mechanism. The question of universal design often emerges when considering the range of target users anticipated to use systems. What is clear from the above is that we must accommodate all ranges of ability wherever possible, ensuring accessibility and inclusion for all.

4 CONCLUSION & FUTURE WORK

Given our recent human-centred research focus on dyslexia and the findings from our fieldwork, the overview of alternative authentication mechanisms, and the emerging WCAG direction, we make several recommendations. First, the life-cycle of authentication needs to be explored in its entirety. It is is naïve to examine only the recall stage, which is admittedly where many of the issues manifest across the entire population. Scrutinising and improving steps across the life-cycle will enhance usability, security *and* accessibility. Second, the implications of the cognitive demand, which extends across a number of challenges faced by individuals, should be acknowledged and accommodated in authentication design. Future work should address the nature of those cognitive elements inherent within the key stage, that of access to systems and services. Finally, full consideration needs to be given to the range of abilities and accessibility needs of individuals with cognitive impairments, especially in the drafting of new authentication standards and guidelines. Methods adopted to research these areas need to be carefully crafted, and be respectful of the needs and potential limitations of participants.

5 ACKNOWLEDGMENTS

We are grateful to our interviewees for opening our eyes to the challenges password authentication poses to those with dyslexia.

REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (Dec. 1999), 40–46. https://doi.org/10.1145/322796.322806

[2] Sarah Andrew, Stacey Watson, Tae Oh, and Garreth W. Tigwell. 2020. A Review of Literature on Accessibility and Authentication Techniques. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '20)*. Association for Computing Machinery, New York, NY, USA, 1–4. https://doi.org/10.1145/3373625.3418005

[3] Mohammadreza Hazhirpasand Barkadehi, Mehrbaksh Nilashi, Othman Ibrahim, Ali Zakeri Fardi, and Sarminah Samad. 2018. Authentication systems: A literature review and classification. *Telematics and Informatics* 35, 5 (Aug. 2018), 1491–1511. https://doi.org/10.1016/j.tele.2018.03.018

[4] CSRC. 2021. Authentication - Glossary | CSRC. https://csrc.nist.gov/glossary/term/authentication Retrieved 23 Feb 2021.

[5] Jane M Flynn and William M Deering. 1989. Subtypes of dyslexia: investigation of Boder's system using quantitative neurophysiology. *Developmental Medicine & Child Neurology* 31, 2 (1989), 215–223.

[6] Marcia Gibson, Karen Renaud, Marc Conrad, and Carsten Maple. 2015. Play That Funky Password! Recent Advances in Authentication with Music. In *Handbook of Research on Emerging Developments in Data Privacy*. IGI Global, 101–132. https://doi.org/10.4018/978-1-4666-7381-6.ch006

[7] Thomas Groß, Kovila P. L. Coopamootoo, and Amina Al-Jabri. 2016. Effect of Cognitive Effort on Password Choice. In *LASER*. USENIX, San Jose, USA, 55–66.

[8] Jordan Hayes, Xiao Li, and Yang Wang. 2017. "I Always Have to Think About It First": Authentication Experiences of People with Cognitive Impairments. In *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '17)*. Association for Computing Machinery, New York, NY, USA, 357–358. https://doi.org/10.1145/3132525.3134788

[9] Anne Kayem. 2016. Graphical Passwords – A Discussion. In *30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. IEEE, Kuala Lumpur, Malaysia, 596–600. https://doi.org/10.1109/WAINA.2016.31

[10] Yao Ma, Jinjuan Feng, Libby Kumin, and Jonathan Lazar. 2013. Investigating User Behavior for Authentication Methods: A Comparison between Individuals with Down Syndrome and Neurotypical Users. *ACM Transactions on Accessible Computing* 4, 4, Article 15 (July 2013), 27 pages. https://doi.org/10.1145/2493171.2493173

[11] E Newby. 1989. Phonological Processing, Verbal and Nonverbal Memory, and Attention in Dysphonetic and Dyseidetic Dyslexia. ERIC Research Report ED308011.

[12] Denise Ranghetti Pilar, Antonio Jaeger, Carlos F. A. Gomes, and Lilian Milnitsky Stein. 2012. Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background. *PLOS ONE* 7, 12 (Dec. 2012), e51067. https://doi.org/10.1371/journal.pone.0051067 Publisher: Public Library of Science.

[13] Karen Renaud, Graham Johnson, and Jacques Ophoff. 2020. Dyslexia and Password Usage: Accessibility in Authentication Design. In *Human Aspects of Information Security and Assurance (IFIP Advances in Information and Communication Technology)*, Nathan Clarke and Steven Furnell (Eds.). Springer International Publishing, Cham, 259–268. https://doi.org/10.1007/978-3-030-57404-8_20

[14] Karen Renaud, Graham Johnson, and Jacques Ophoff. 2021. Accessible Authentication: Dyslexia and Password Strategies. *Information & Computer Security (To Appear)* (2021).

[15] Jeremiah D Still, Ashley Cain, and David Schuster. 2017. Human-centered authentication guidelines. *Information & Computer Security* 25, 4 (2017), 437–453. https://doi.org/10.1108/ICS-04-2016-0034

[16] Ignacio Velásquez, Angélica Caro, and Alfonso Rodríguez. 2018. Authentication schemes and methods: A systematic literature review. *Information and Software Technology* 94 (Feb. 2018), 30–37. https://doi.org/10.1016/j.infsof.2017.09.012

[17] W3C. 2015. Cognitive Accessibility User Research. https://www.w3.org/TR/coga-user-research/#dyslexia Retrieved 23 Feb 2021.

[18] W3C. 2016. Gap Analysis Summary - Cognitive Accessibility Task Force. https://www.w3.org/WAI/GL/task-forces/coga/wiki/Gap_Analysis_Summary Retrieved 23 Feb 2021.

[19] W3C. 2018. Coga Task Force. https://www.w3.org/WAI/GL/task-forces/coga/ Retrieved 23 Feb 2021.

[20] W3C. 2020. Understanding Success Criterion 3.3.7: Accessible Authentication. https://www.w3.org/WAI/WCAG22/Understanding/accessible-authentication Retrieved 23 Feb 2021.

[21] W3C. 2020. Web Content Accessibility Guidelines (WCAG) 2.2. https://www.w3.org/TR/WCAG22/ Retrieved 23 Feb 2021.

[22] W3C. 2021. Cognitive Accessibility User Research: W3C Editor's Draft 22 February 2021. https://w3c.github.io/coga/user-research/ Retrieved 23 Feb 2021.

[23] Stephan Wiefling, Tanvi Patil, Markus Dürmuth, and Luigi Lo Iacono. 2020. Evaluation of Risk-Based Re-Authentication Methods. In *ICT Systems Security and Privacy Protection (IFIP Advances in Information and Communication Technology)*, Marko Hölbl, Kai Rannenberg, and Tatjana Welzer (Eds.). Springer International Publishing, Cham, 280–294. https://doi.org/10.1007/978-3-030-58201-2_19

[24] Debby Zambo. 2004. Using Qualitative Methods to Understand the Educational Experiences of Students with Dyslexia. *The Qualitative Report* 9, 1 (March 2004), 80–93. https://nsuworks.nova.edu/tqr/vol9/iss1/5 Retrieved 16 Jan 2021.