Designing authentication with seniors in mind

Karen Renaud
Kenneth C. Scott-Brown
Andrea Szymkowiak

Designing Authentication with Seniors in Mind

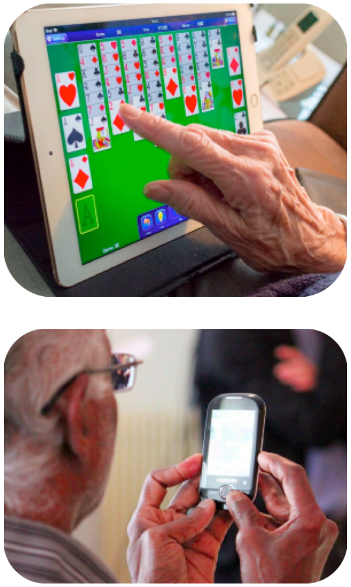

Figure 1: Seniors enjoying their digital devices (Images from Pixabay by Sabine van Erp & Jérôme Choain)

Karen Renaud
Kenneth Scott-Brown
Andrea Szymkowiak

Abertay University
Dundee, UK DD1 1HG, UK
k.renaud@abertay.ac.uk
k.scott-brown@abertay.ac.uk
a.szymkowiak@abertay.ac.uk

Abstract

Developers typically adopt perceived best practice, and in the case of authentication this means password security. However, given the wide range of technical solutions available and the diverse needs and limitations of older users, we suggest that the default adoption of electronic "username and password" authentication may not be 'best practice' or even good practice. This paper highlights some challenges faced by three seniors, each of whom has multiple age-related disabilities and concomitant life challenges. The result is that they cannot authenticate themselves when they need to access their devices and accounts. We conclude by suggesting a number of research directions calculated to address some of these challenges and promote inclusive design and allow for diverse user authentication.

Author Keywords

Authentication; Seniors; Accessibility;

ACM Classification Keywords

• Human-centered computing~Accessibility theory, concepts and paradigms
• Human-centered computing~Accessibility design and evaluation methods.

Introduction

The EU commission states that 80 million people in the EU are affected by a disability. As the EU population ages this number is predicted to increase to 120 million by 2020. There is a need to design for accessibility so that the elderly can participate equally and actively in society [6]. The UN Convention on the Rights of Persons with Disabilities contains accessibility obligations [20] and requires Member States to accommodate those with disabilities. It is almost 10 years since they published this manifesto, but there is not much evidence that it has been taken to heart, especially when designing authentication mechanisms.

We would like to introduce three *fictitious* senior citizens to illustrate the difficulties they are likely to face when interacting with technology and to highlight their needs.

Vera is 81 years old and lives independently, despite a number of health issues. Her metabolism has slowed to such an extent that her fingers are always cold. She is more or less housebound due to severe arthritis. She can hear with her brand new hearing aid, but experiences difficulty remembering things these days.

Vera's proudest possession is her iPad, with her iPhone a close second. She is having some problems though: she has managed to lock herself out of her iPhone and needs to sign into her iCloud account on her iPad to reactivate it. Her fingers are too cold for the fingerprint reader to pick up, and she finds that she has forgotten the PIN. She eventually finds the bit of paper she wrote it on. She now needs to sign into iCloud, with its 14-character password. This is extremely frustrating because she forgets where she is halfway through as she types it in, and finds that holding the Shift key down while she types is hard with her arthritic fingers. Actually, she only needs to tap it, but she is erroneously applying her "typewriter" mental model to the situation. She subsequently also gets locked out of her iCloud account. She has to wait two weeks for her daughter to come and visit her before the situation can be resolved.

John, 75, receives an email from what claims to be his email provider, asking for credentials. The phisher takes over his email account and he cannot figure out how to contact Microsoft. A cleaner arrives, and John has to ask for her assistance to resolve the problem. This takes 2 hours and the cleaner has no time to clean his apartment. She also feels uncomfortable because she now possesses personal details belonging to her client.

Jo is 90 years old, with early stage dementia, depression and delirium. Jo can physically navigate the home but is unable to operate a TV remote or a telephone. Judged fit to be discharged from hospital, Jo is sent home and is still expected to run a current account with a debit card, even though housebound. Jo asks a neighbor to draw money, and he does this, but also helps himself to £100 and claims he delivered all the money. Because of the dementia, no one believes Jo's version of the event and the neighbor gets away with the theft.

These vignettes, loosely based on the authors' personal contacts, demonstrate how the *de facto* authentication mechanisms of the 21st century are failing to meet the needs of our older population. Our seniors have multiple health issues and are often lonely and poorly supported. The industry's focus on designing mechanisms with the able-bodied in mind, under the assumption that the end user will be familiar with the mechanisms and dangers of the digital world, leaves seniors frustrated, excluded and vulnerable to hacking attacks and fraud.

Authenticating someone at a distance, especially digitally, is nontrivial. The digital world generally makes use of a shared secret to achieve this but, as we shall show, this is suboptimal, especially for our seniors.

Consider the advice usually given to password creators: (1) create a password that is essentially nonsense, that no one can guess, and (2) don't write it down [11]. Even for young people with agile minds this is taxing. Yet this advice is even more difficult to follow if you are aging and your memory is not as sharp as it used to be. Other password advice mandates complexity, which makes passwords hard to input with arthritic fingers, even if they can be remembered.

In this paper, we outline the challenges faced by senior citizens needing to authenticate themselves. We then discuss a number of research opportunities that ought to be considered when designing an accessible authentication mechanism that will not exclude, alienate or render senior users vulnerable to exploitation [1, 14].

Challenges to Seniors

Inaccessible Interfaces

Many of the elderly of today did not use computers during their working lives. This means that they have no mental models to match the interfaces they have to engage with when they used the latest technologies. Moreover, technology changes much faster than they are comfortable with, often leaving them feeling disoriented. It takes them longer to process changes and the speed of change means them feeling as if they are never catching up.

Inaccessible Authentication

The most widely-used authentication mechanism is the password, perhaps because of it was the first mechanism used to control access to computers [13] or because the choice of a password represents the least effort for developers [18]. Yet many people struggle with passwords, and the aged find them particularly troublesome [8]. Design guidelines for senior-sensitive design cannot be used to inform authentication design because they maximize feedback and error correction [12]. Because authentication is security-related, this conflicts with good practice.

Passwords rely on the ability to remember a long nonsense string. This ability severely declines as we age [19]. Passwords arguably fail the accessibility test when the user base includes older users.

Some researchers have designed picture-based passwords in order to make authentication less burdensome in terms of memory [16, 17]. Others have exploited the fact that music memory is more permanent and erodes less easily than memory of character strings [7]. These have not enjoyed widespread uptake.

Some devices are now routinely released with inbuilt fingerprint or face biometric readers. Our first vignette shows that this seemingly effortless mechanism fails for many users, due to age-, disability- or health-related infirmities [3].

The other alternative is the use of a token, something the user owns. However, dementia and Alzheimers, diseases that strike predominantly older users, will make them lose or misplace these [10]. Moreover, many tokens are used in conjunction with a PIN or password, which is also likely to be forgotten.

Supported Living

Many seniors become increasingly reliant on family members, merely to get through their usual day-to-day lives. The overwhelming majority of such carers would not dream of exploiting their relatives but there are exceptions [5].

However, many do not have a family member or trusted friend to help them. Many do need help authenticating, especially now that governments routinely deposit pensions and benefits into people’s bank accounts [4]. The question is how those who need support elicit help without opening themselves up to fraud and theft.

Seniors are familiar with hard cash, not with using a card to pay for goods and services. Society has moved to card payments and online banking, and are often given no choice in the matter [4]. Yet age-related infirmities and mobility issues are a major obstacle. How does an older person draw cash from the bank when they cannot get to the bank themselves? The banks do not offer any mechanisms to support this. When people are unable to access their own money, they are left feeling helpless and disempowered. Even worse, they are forced into violating the terms of use of their account in order to get cash, eliciting assistance from helpers, friends and family. Any subsequent fraud will be blamed on the account holder rather than the fact that a system has not been designed to accommodate their limitations.

Why Authenticate?

Before we talk about solutions, we need to take a close look at exactly what the purpose of authentication is. Essentially, authentication confirms that the person claiming identity has a right to claim it. Kent and Millet say there are two reasons for such confirmation being important: (1) Accountability, and (2) Authorization [11].

In the first case, authentication is carried out so that users can be held accountable for their actions while using the system. In the second case, people are permitted to carry out particular actions based on their confirmed identity: they are *authorized* to do so.

Does either of these justifications apply to Vera using her iPad? Vera is not accountable to anyone else for what she does to her own device. By dint of ownership she has no need to be authorized. It seems that a third reason for authenticating is coming into play here: preventing 3rd party usage. If someone were to steal the iPad, they would not, theoretically, be able to use it because authentication is required.

In other words, Vera is being required to authenticate multiple times a day just in case someone steals her iPad. The cumulative cost to Vera, and the frustration that results if she is locked out after three tries, is not factored into the design of the mechanism. A more usable solution would allow more attempts, or allow authentication by proxy where a trusted family member could help her remotely if she forgets her password.

If accessibility were taken seriously, the government would not force Jo to engage with a digital world when she is cognitively and physically unable to do so. Those who provide pensions are, by definition, dealing with some of the most vulnerable members of society. More flexibility and indeed, genuine accessibility, would not go amiss.

The UN's Article 9 mandates the following with respect to assuring accessibility for the disabled[1] (we only report those items relevant to authentication). The identification and elimination of obstacles i.e. to:

(1) provide information, communications and other services, ***including electronic services*** and emergency services,

(2) monitor the implementation of minimum standards and guidelines for the ***accessibility of facilities and services open or provided to the public,***

(3) provide training for stakeholders on ***accessibility issues*** facing persons with disabilities,

(4) ***promote other appropriate forms of assistance*** and support to persons with disabilities to ensure their access to information,

(5) promote access for persons with disabilities to new information and communications technologies and systems, ***including the Internet,*** and

(6) promote the design, development, production and distribution of accessible information and communications technologies and systems at an early stage, ***so that these technologies and systems become accessible at minimum cost*****.**

There is little evidence, when one listens to the experiences and anecdotes reported by the elderly, that these guidelines are being taken note of and adhered to.

Opportunities

We now describe some design recommendations for further research when implementing accessible authentication technology for the elderly.

Authentication – Accessible Implementation

Password requirements that mandate complexity (upper case, lower case, digits and special characters) are particularly problematical. This is so especially when they encourage the invocation of the incorrect mental models, such as the example of Vera holding down the shift key, instead of tapping it. Mandating inclusion of special characters requires seniors to switch soft keyboards, something they have no mental model for. Moreover, many systems obfuscate password entry. Age-related short-term memory decline [15] leads to people forgetting where they are in terms of entering the password. This leads to multiple entry attempts, and possibly getting locked out.

[1] https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/article-9-accessibility.html

Authentication – At Home, But Not Alone

When people authenticate on their own devices they are not being authenticated to hold them accountable, or to authorize them. It is being carried out to protect their devices in the case of theft. Bonneau *et al*. [2] argue for technological "smarts" to be used to augment passwords in order to achieve a more reliable authentication.

For example, a more innovative way to authenticate Vera would permit device usage from one particular network or location without deliberate authentication being required. Proof of identity, by engaging in authentication, could only be required if the device is used from a different location.

When authentication is unavoidable, such as when money is being drawn from a bank account, or a purchase is being made from their device, innovation could deliver more accessible solutions.

For example, the older person could nominate a trusted person to carry out a proxy sign-in on their behalf: assisted sign in. Social support has been shown to be a powerful motivator in terms of modern technology usage [9]. Clearly the older person and the trusted "other" would pre-arrange a protocol in advance. This might be a phone call, or the older person being identified by a person at the bank branch, and then contacting the trusted other.

People are told never to share their PINs, but the issue of housebound people being unable to draw cash is not considered. Banks ought to offer a mechanism for one-time expiring PINs to be issued, linked to a particular withdrawal amount. This would allow the person to ask someone else to withdraw cash for them, without being worried about the person emptying their account, or reusing the PIN multiple times.

If the senior uses their own iCloud (or equivalent cloud storage service) account from their home location, an assisted login would also free them from the burden of password retention.

Conclusion

In this paper, we have sought to highlight the challenges facing the elderly who have multiple age-related disabilities. We discuss opportunities for research to address the identified issues. Although the UN Human Rights charter mandates accessibility, there is little evidence that this human right is being enjoyed by the elderly. It is important for designers to start thinking about this market, especially because it is growing at an unprecedented rate and will incorporate future seniors, including ourselves.

References

1. Anon. 2018. FRAUD ALERT: Elderly Harrogate woman conned out of £9,200 in courier fraud. https://northyorkshire.police.uk/news/courier-fraud-alert-elderly-harrogate-woman-conned-9200/ (Accessed 20 April 2018)
2. Bonneau, J., Herley, C., Van Oorschot, P.C. and Stajano, F., 2015. Passwords and the evolution of imperfect authentication. Communications of the ACM, 58(7), pp.78-87.
3. bromba.com. Bioidentification: Frequently Asked Questions. Accessed 26 April 2018 http://www.bromba.com/faq/biofaqe.htm
4. Citizens Advice Bureau. undated. Payment of benefits and tax credits. https://www.citizensadvice.org.uk/benefits/benefits

-introduction/payment-of-benefits-and-tax-credits/ (Accessed 20 April 2018)

5. Doherty, S. 2018. Obsessive boyfriends, child abusers and the woman who defrauded her mother - Kent criminals who abused positions of power and trust. 12 April. https://www.kentlive.news/news/kent-news/kent-criminals-who-despicably-abused-1450430 (Accessed 20 April 2018)

6. EU. Commission proposes to make products and services more accessible to the disabled persons. http://europa.eu/rapid/press-release_IP-15-6147_en.htm (Accessed 20 April 2018)

7. Gibson, M., Renaud, K., Conrad, M. and Maple, C., 2009, September. Musipass: authenticating me softly with my song. In Proceedings of the 2009 workshop on New Security Paradigms Workshop (pp. 85-100). ACM.

8. Helkala, K., 2012, August. Disabilities and authentication methods: Usability and security. In Availability, Reliability and Security (ARES), 2012 Seventh International Conference on (pp. 327-334). IEEE.

9. Hill, R., Beynon-Davies, P. and Williams, M.D., 2008. Older people and internet engagement: Acknowledging social moderators of internet adoption, access and use. Information Technology & People, 21(3), pp.244-266.

10. Ishii, H., Kimino, K., Aljehani, M., Ohe, N. and Inoue, M., 2016. An Early Detection System for Dementia Using the M2 M/IoT Platform. Procedia Computer Science, 96, pp.1332-1340.

11. Kent, S. and Millet, L. 2003. Who Goes There. Authentication Through the Lens of Privacy. The National Academies Press. Washington.

12. Kurniawan, S. and Zaphiris, P., 2005, October. Research-derived web design guidelines for older people. In Proceedings of the 7th international ACM SIGACCESS Conference on Computers and Accessibility (pp. 129-135). ACM.

13. Morris, R. and Thompson, K., 1979. Password security: A case history. Communications of the ACM, 22(11), pp.594-597.

14. Mulligan, S. 'Despicable' fraudsters who targeted elderly victims sentenced. http://www.sthelensstar.co.uk/news/16167215._Despicable__fraudsters_who_targeted_elderly_victims_sentenced/ (Accessed 20 April 2018)

15. Murphy, D.R., Craik, F.I., Li, K.Z. and Schneider, B.A., 2000. Comparing the effects of aging and background noise on short-term memory performance. Psychology and Aging, 15(2), p.323.

16. Renaud, K., 2006. A visuo-biometric authentication mechanism for older users. In People and Computers XIX—The Bigger Picture (pp. 167-182). Springer, London.

17. Renaud, K. and Ramsay, J., 2007. Now what was that password again? A more flexible way of identifying and authenticating our seniors. Behaviour & Information Technology, 26(4), pp.309-322.

18. Renaud, K. and Maguire, J., 2013, May. Shrinking the Authentication Footprint. In EISMC (pp. 2-11).

19. Salthouse, T.A., 2003. Memory aging from 18 to 80. Alzheimer Disease & Associated Disorders, 17(3), pp.162-167.

20. UN. 2009. Convention on the Rights of Persons with Disabilities (CRPD) https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html (Accessed 20 April 2018)