Usable biometrics for an ageing population[1]

M. Angela Sasse & Kat Krol

Department of Computer Science, University College London (UK)

Abstract

In this chapter, we examine the implications of ageing for the usability of biometric solutions. We first set out what usability means, and which factors need to be considered when designing a solution that is 'usable'. We review usability successes and issues with past biometric techniques, in the context of a set of solutions, before considering how usability will be affected for ageing users because of the physical and cognitive changes they undergo. Finally, we identify the opportunities and challenges that ageing presents for researchers, developers and operators of biometric systems.

1 Introduction

In this chapter, we examine how ageing affects human interaction with biometric systems. We focus on the ability and willingness of older users to engage with advanced technologies, and use them successfully. Ageing can change physical and behavioural characteristics, and this can impact performance – see the chapter by Lanitis et al. in this volume; in this chapter, we focus on the change in general physical and cognitive capabilities, and how this impacts the ability to interact with the systems in which biometric recognition is embedded. If older users find it hard to present their biometrics correctly, or find the behaviour required to present unacceptable, this can lead to exclusion – this and other broader ethical and social implications of the issues we observe are examined in detail in Chapter 3 (Rebera & Mordini, this volume).

We conclude that the current usability challenges that biometrics presents for elderly users are not insurmountable – they can be overcome by systematic application of

[1] A version of this paper appeared in Fairhurst, M. (ed.): Age factors in biometric processing. http://www.theiet.org/resources/books/telecom/age_factors.cfm?origin=/

human-computer interaction knowledge and principles, and a determined empirical effort to improve performance through testing and adaption. Once this is achieved, biometric technology has the potential to be a key enabler of access to new technology and services for elderly users, who struggle with current security mechanisms such as passwords and CAPTCHAs. Biometric technology that can be adapted to meet requirements of older users and performs reliably would transform the interaction of older users with technology.

2 What is usability?

Usability is defined by the International Organization for Standardization (ISO) as *"The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use."* (ISO 2010)

So to design a usable product or system, the design needs to fit with the characteristics of the target users, their goals and tasks, and the physical and social context in which they interact with that technology. We examine what each of these characteristics means for usability of biometrics.

2.1 User Characteristics

From ergonomics, usability has inherited the notion of general and specific user characteristics. *General user characteristics* are physical and mental characteristics shared by all – or rather, nearly all – humans, such as having 2 arms and 10 fingers, being able to see, hear and speak. But there are 3 reasons why the idea of general physical and mental characteristics is problematic.

1) Within the general characteristics, there are ranges. Taking body height as an example, the difference between the tallest (2.51m) and shortest (0.54m) living person is nearly 2 meters. These are of course extremes, and traditional ergonomic design practice was to design the physical aspects of systems to accommodate 95% of the population. Variations that can pose particular challenges for biometric systems include those in skin and eye colour. There are also ranges in perceptual capabilities – such as visual acuity and hearing – and mental ones – speed of processing, number of items a person can recall.

2) Even though the characteristics are supposed to be general, not all humans fit the template: some are born without certain limbs or digits, other may lose them during their lifetime because of accidents or illness. Whilst a few decades years ago, humans thus affected were labelled as 'disabled' and not expected to participate in many work or leisure activities (such as travel) in many parts of the world, we now a regard them as differently abled, and adapt the physical environment to allow them to participate. This notion extends to technology – the principle of *universal access* states that technologies must be designed so they do not exclude users with disabilities. This is enshrined in both the ISO usability standard, and many countries compel public and commercial sector organisations to design facilities and technologies that allow access.
3) Some characteristics change during the lifetime of a human – human grow from 'Fetus into Man' (Tanner, 1989) – in terms of height, physical maturity is reached around age 20, but different body tissues mature at different rates. Body height declines from the age 50 onwards due to bone shrinkage, and the acuity of sight and vision can start to decline even earlier. As we shall see later, the age-related changes can affect both biometric characteristics themselves, and make it more difficult to operate the systems through which users interact with them. Lanitis et al. (in this volume) conclude that ageing affects the biometric templates of all biometric traits, in different ways.

Given this level of variation, the notion of *general human characteristics* that a biometric solution could build on is starting look problematic – at least for systems that need to accommodate a large, heterogeneous user population – for example, in a national context, biometrics are added to passports.

The more a system can be targeted to a specific user group and its capabilities, existing experiences, and expectations, the more usable it will be. With homogeneous user populations, solutions can be developed to match the *specific user characteristics* that group – if we design a system for , say, Formula 1 drivers, we would have to have to accommodate few of the variations above – those resulting ethnic differences being a notable exception.

Sometimes, making a system accessible for differently abled or elderly users can result in improved convenience that appeals to users beyond the target population.

The television remote control was originally developed for users with reduced mobility, who had difficulty getting up to change the television channel. But the convenience it offered was so attractive to able-bodied users that Robert Adler from Zenith developed the prophetically named ‘lazy bones’ version for the wider consumer market, creating several generations of couch potatoes in the process.

Making a system senior-friendly and improving navigation performance among younger users as a side-effect has also been documented in Web usability. In their study, Chadwick-Dias, McNulty and Tullis (2003) show that after a redesign of a Website in line with the feedback received from older users, user performance improved for both younger and older participants in a subsequent study.

Other adaptions made for those with reduced capabilities do not appeal beyond the target user group. A good example is when consumer technologies are made simpler or bigger. Many older users find modern smartphones too complex to understand, and too small to operate effectively, so mobile phone companies have started to offer phone with larger displays and buttons that offer only voice calls. These ‘simple’ phones with reduced functionality will not appeal to a wider user group of younger users who want to access email and Facebook while on the move.

Whenever possible, designers must fit the system to the capabilities of the user, and not vice-versa. In usability, fitting the user to the system, through the use of education and training for example, is always a secondary option, which is only deployed when technology cannot be adapted to human users, or the cost of doing so would outstrip the utility of the system.

2.2 User Goals

Human behaviour is largely goal-driven. Whilst there are some users for whom playing with technology is an enjoyable pastime, most use it in pursuit of work or private goals. Most older people who become silver surfers do so because they want to stay in touch with their grandchildren, clear out the garages, or find health information or cheaper medication online. Users carry out *tasks* they see as steps towards achieving those goals. Goals can be composed into *primary tasks* (chat to my grandchild via Skype, sell my collection of motorbike tools on eBay); but in the course of these, users are confronted with a number of *secondary* or *enabling* tasks:

(e.g., creating a Skype or eBay account). Users can understand that these are necessary, but try to get them done as quickly as possible, so they can return to the primary tasks on the path towards achieving their goals – meaning they will not take pride in doing it well, or see it as something worth investing time and effort in. Security is a secondary task – users don't want to give it much time or attention. If it secondary tasks become a noticeable drain on resources, or disrupts the path to the primary goal, users will resent it. If users are not able to complete a security task at all (something that happens to many confronted with a CAPTCHA, see section 4.2) they are barred from the service altogether – a Lose-Lose result for customers and service providers alike.

Whether a security mechanism "fits" with primary task depends on a number of factors:

1) The frequency with which the mechanism is used. Adams & Sasse (1999) found that many people can manage relative complex passwords if they use them several times a day – with frequent usage, retrieval form memory becomes automatic.
2) The number of similar credentials or actions. Even frequently used passwords are likely to be confused by users who have many similar memory items, or in the first couple of days after changing it.
3) Time taken to complete primary and security task. The time and effort associated with a secondary task has to be proportionate to the primary task – see also the Compliance Budget below. Sasse & Brostoff (2000) found that the introduction of a service graphical authentication mechanism reduced access to the system by 60% compared to passwords (which users previously said they did not like), because it took too long to authenticate.
4) The disruptiveness of the secondary task. The way in which the security mechanism fits with the primary task is crucial – if it interrupts the user in a critical time of executing the primary task, or competes for the same physical and mental resources, it will affect performance and perception.

   People make implicit cost-benefit assessments as they go through life. If the perceived effort involved in a secondary task exceeds the perceived benefits, they experience what Beautement et al. (2008) call *friction*. Most users recognise that security mechanisms have some benefit for them or their organisation, but since they usually rate the risk differently from security experts, their perception of whether it is worth making that effort is different. Herley (2009) argues that users' assessment of risk makes more sense from an economic point of view than that of security experts – who *"value users' time at zero"* and ignore the workload and disruption that cumbersome and complex security mechanisms create.

Most employees and consumers now have to comply with a multitude of security mechanisms – especially around authentication. Beautement et al. describe how, if there are several such tasks, friction accumulates and users approach their *compliance threshold*. When close to their compliance threshold, users will try to shortcut the security tasks (e.g., by choosing *c@t1c@2c@3c@t4* when told they have to have a 12 character cryptographically strong password). Such actions often reduce or cancel the effectiveness of the security mechanism. As described in 4.1, the load of knowledge-based authentication has become such that many users now suffer from authentication fatigue, and this presents an opportunity for well-designed biometric solutions.

2.3 Context of Interaction

Users interact with a system in a physical and social context, which can create constraints in terms of usability. For instance, as we discussed above, many users succeed in recalling and entering a long and complex, but frequently used password in a traditional office environment. Entering the same password on a touchscreen will take significantly longer, and fail more often, even with frequent use. The same voice recognition can work well in quiet environments, but fail when the user is in a place with high background noise. Physical and social environments constraints also affect how secure a mechanism is: whilst receiving entry feedback from your iPhone may improve accuracy, it becomes a threat when you have to enter it many times with colleagues looking over your shoulder.

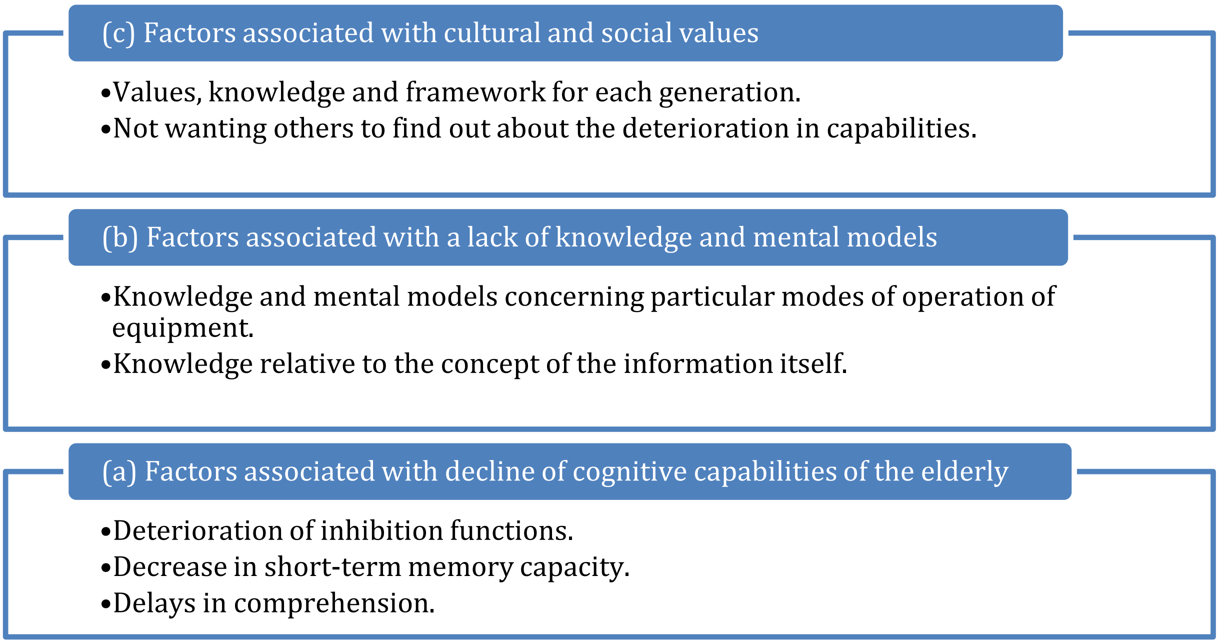
2.4 Implications for design

The implications of the usability framework present a challenge to the designers of security systems today: they are used to choosing from a relatively small set of standard mechanisms. For authentication purposes, for instance, passwords continue to be widely used, even though the usability problems and impact on personal and organisational productivity have been documented (Adams & Sasse, 1999; Inglesant

& Sasse 2010). A ‘usable security’ authentication solution would mean selecting a mechanism that creates minimal physical or mental workload for users, does not disrupt them in the execution of their primary tasks, and can successfully operate and be operated in the physical and social context. Biometrics have the potential to offer reliable authentication with low physical and mental workload - especially if the biometric sample for recognition can be captured as a by-product of the activity users perform in pursuit of their primary goal (see section 4.1). If designers think along these lines, it would particularly benefit elderly users because it would also minimise the need to learn or remember anything about the system (see next section).

3 The impact of cognitive ageing on the use of technology

Akatsu and Miki (2004) stress that for a long time usability for elderly focussed on assisting with visual and physical impairments by increasing contrast, font size or making buttons easier to press. However, they postulate that in order to increase usability, it is necessary to also include cognitive considerations. They suggest a three-layer model addressing cognitive ageing and how it influences elderly people’s use of technology.



(c) Factors associated with cultural and social values

- Values, knowledge and framework for each generation.
- Not wanting others to find out about the deterioration in capabilities.

(b) Factors associated with a lack of knowledge and mental models

- Knowledge and mental models concerning particular modes of operation of equipment.
- Knowledge relative to the concept of the information itself.

(a) Factors associated with decline of cognitive capabilities of the elderly

- Deterioration of inhibition functions.
- Decrease in short-term memory capacity.
- Delays in comprehension.

Fig. 1: Ease of use and cognitive ageing: A three-layered factor model by Akatsu & Miki, 2004.

3.1 Deterioration of cognitive capabilities

With age people's ability to acquire new skills declines, they struggle when they have to master a new skill, particularly if it has a high level of complexity. In what follows, we describe the five main signs of age-related cognitive decline and their impact on interaction with technology.

Longer reaction times

As we age our reaction times become slower. It is a well-researched phenomenon and its impact has been studied in many areas, most notably in driving (e.g., Makishita & Matsunaga, 2008; Cantin, Lavallère, Simoneau & Teasdale, 2009).

Related to longer response times is the elderly's difficulty in collecting information quickly. This can be due to the fact that the space dimension of perception shrinks with age. Space dimension of perception is the amount of information that can occupy a person's attention at any one time (Worcester, Loustau & O'Connor, 1990). This quantity of information is subject to age-related changes and young people are able to absorb more information than older ones. Studies in the field have shown that younger people scored better when presented with unfamiliar information accompanied by distractions than the elderly. Nevertheless, elderly participants performed better when they were given less but familiar material with no distractions present (Botwinick, 1984). For that reason, it is crucial that the elderly are given enough time when interacting with a system. In a study by Akatsu and Miki (2004), some elderly participants experienced timeouts when they took too long to complete the experimental tasks on an ATM. A timeout meant that they needed to start the task from the beginning. In comparison with university students, the elderly in the study required twice as long for the procedure of a withdrawal and three times as long for a fund transfer.

Attention

There are also significant changes in attention, especially in selective attention. Younger people have been shown to perform better in selective attention tasks than younger. Rogers (2000) showed that three factors reduce this difference: experience, cues and the heterogeneity of target-distracting objects.

Memory decline

Cross-sectional and longitudinal studies have shown a decline in working and episodic memory (Hedden & Gabrieli, 2004). With age, there are significant declines in abilities such as the encoding of new memories and the processing speed of new information. There is also a decline in working memory which is the simultaneous short-term maintenance and manipulation of information involving executive processes.

Usability studies involving cross-generational comparisons also showed that older participants received lower scores for verbal memory than younger participants (Ziefle & Bay, 2006). In a Learning and Memory Test, younger participants received an average score of 13.3 out of 15 while older participants 11.4. This difference was found to be statistically significant (p=.005). Memory ability and age were found to be negatively correlated (r=-.46, p=.008).

Research by Johnson, Reeder, Raye & Mitchell (2002) has shown that the elderly have a deficit in information refreshing, that is, in the simple reflective operation of thinking of a just-presented item. The researchers stress that this can have an impact on other age-related cognitive phenomena. Activated but irrelevant items persist more for older than younger people. Older adults might lack the ability to suppress the activation of task-irrelevant information (Hasher, Zacks & May, 1999). Johnson et al. (2002) suggest that the failure to suppress irrelevant information may be related to the failure to activate relevant information. This is a possible explanation for why older participants sometimes become lost in system menus (Akatsu & Miki, 2004) or struggle when confronted with detailed information (Chadwick-Dias et al., 2003).

Spatial abilities

Spatial ability comprises of spatial memory and spatial scanning. Spatial memory is responsible for the mental visualising of spatial location of some elements. Spatial scanning is the action of visually scanning through available information. With age, spatial abilities decrease in precision and quickness. In order to measure spatial abilities of different age groups, Ziefle and Bay (2006) used the paper-folding test in their study on the usability of mobile phone menus. While the younger participants had a mean performance of 13.4 (SD=3.5) out of 20, the older ones 9.6 (SD=3.6). This difference was found to be statistically significant (p=.004). A correlation between spatial abilities and age showed that spatial abilities decrease as a function of age (r=-.53, p=.002).

In a study on navigation through a menu of interactive TV, Obrist et al. (2007) found that elderly participants explored the interface as fast as younger ones but they lacked accuracy. Elderly participants struggled with the use of navigational keys. They were always slower in viewing, searching and finding of information than younger participants. The authors attributed it to elderly people not being familiar with current conventions of information presentation and navigation. They also struggled due to visual impairments when the colour contrast was not high enough or the font size too small.

3.2 Lack of knowledge and mental models

Mental models are the user's mental representations of how a particular system works and how it is structured (Gentner & Stevens, 1983). Mental models are formed through increasing expertise and combine prior experience, cognitive schemata and problem-solving strategies (Johnson-Laird, 1983). Age and lack of experience make it less likely for users to develop a correct and useful model of a system (Calero-Valdez, Ziefle, Alagöz & Holzinger, 2010). Research has shown that a good mental model of a system improves user performance. In a study on a small-screen diabetes assistant, Calero-Valdez et al. (2010) found that having a simplified spatial representation of a device menu improves user performance. Even those having an inaccurate mental model performed better in the experimental tasks than those who did not have a mental representation of the system at all. The study also showed that previous experience with similar devices matters. Experience with mobile phones was significantly correlated with the quality of the arranged model of the diabetes assistant (r=-.43).

3.3 Cultural and social values

Within the realm of the cultural and the social, we identified three major factors that influence elderly people's interaction with biometric systems. These are (i) the tension between generations, (ii) habits and experience and (iii) beliefs and convictions.

Tensions between generations

Akatsu & Miki (2004) reported that some of their participants mentioned that they did not want to be a nuisance to others and did not want people around to become aware of their deteriorated cognitive capacities. Participants in a study by Sayago (2006) reported that the younger generation discouraged them from using computers. Some were told they might break them or delete important information.

Habits and experience

Elderly people often struggle with cash machines, thus they decide to go to a teller. Studies show that the older the customer, the more likely they are to go to a teller instead of using a cash machine (Akatsu & Miki, 2004).

When it comes to experience, studies have shown that elderly people do not realise the shortcomings of computer systems as younger people do. For example, in the ATM study by Akatsu and Miki (2004), a voice message prompting the user to enter their name was given at a time after they already did so. Nevertheless the elderly often started entering their name again, although it was already entered in the field there. A younger user would have realised that there is a glitch in the software and the machine did not register that they had already entered their name, but an elderly person did not question the system and complied with the request.

The elderly are used to more personal service, to speaking to a cashier, getting things explained and their questions answered. Nowadays, the industry is pushing towards automation of interactions in banking and retail. Manned tills gradually disappear and customers are encouraged to use automated check-outs. One might think it is becoming more anonymous but this is not entirely the case. Customers are anonymous in the sense that they do not have face-to-face interactions with the cashier, but they are not anonymous in the sense that the shop or the bank do not know who has just used their services. Because of identity verification in a bank or loyalty cards in a supermarket, these institutions have more information about their customers than they did in the past. Thus, elderly users are more used to face-to-face interaction, and they are likely to find the cold automated way of doing things unfriendly and invasive in the way that gathered information about their habits is stored and processed by machines rather than remembered by the shopkeeper who knew them by their first name.

Another factor here is the fact that elderly people crave human contact. If they have the option to choose between using a system that is difficult to understand and has too much information or a friendly helpful cashier providing them with all necessary information, they will always decide for a cashier. And this is true for young users too. Our recent study showed that in a work context employees are more likely to call up their helpdesk if they feel that looking for information online is not going to give them the answers quickly. If a service provider's aim is to automate their services they have to make these systems highly usable and make them have a clear advantage over manned counterparts.

While younger users tend to be more confident and would blame the system for hold-ups, older users would tend to blame themselves for failing to accomplish a task. In general, older users tend to be more patient and compliant with what the system asks them to do. Studies have shown that older users take longer to complete a set task because unlike digital natives they read all the information on the screen (e.g., Groff, Liao, Chapparo & Chapparo, 1999; Chadwick-Dias, McNulty & Tullis, 2003). For that reason, instructions given should be concise to be comprehensible and quick to read for both younger and older users.

Beliefs and convictions

Older adults are more likely to exhibit computer anxiety (Ellis & Allaire, 1999). A range of studies has shown that the elderly do not understand the benefits of use of computers (Czaja & Sharit, 1998; Melenhorst, Rogers & Caylor, 2001) and think that the benefits from using technology outweigh the effort that has to be put into learning how to use it (Holzinger et al. 2008). In the case of biometric systems not only the unfamiliarity with technology could be a reason for resenting the use of biometric systems but also the association elderly users could have of fingerprints with criminality (Davies, 1994).

3.3 Behavioural implications

Studies into Web usability and age have come up with lists of what is different about the elderly in terms of their interaction with devices. Chadwick-Dias, McNulty & Tullis (2003) show that elderly users

- are more cautious to click on links,
- sometimes repeatedly click widgets that are not links,
- access highly detailed information and never move beyond it,
- struggle with Web terminology and jargon,

- spend more time to read text and instructions,
- struggle to understand their location and path and
- have difficulty with window management, scrolling and tabbed navigation.

3.4 Improving elderly users' interaction with biometric systems

The cognitive challenges in the use of biometrics that we have highlighted can be attributed to two main factors *ability* and *attitude*. Although not much can be done about the deteriorating cognitive capacities that impact ability in elderly users, the interfaces can be designed in order to make the interaction more intuitive and pleasant. The cognitive decline is a well-researched topic and we briefly highlighted its impact on the interaction with technology in Section 3.1. There is an increasing body of research on how the elderly use technology and there are a number of guidelines for making interfaces senior user friendly (Hodes & Lindberg, 2002). At the same time, attitudes towards technology have to do with beliefs and convictions which are shaped by preferences and experience. We suggest that the following four measures could help diminish the impact of cognitive decline and have a positive impact on changing attitudes towards biometric systems.

Training and feedback improve interaction

Research has shown that exposure, training and practice can make the elderly more successful in interacting with biometric systems. Theofanos et al. (2006) showed that when receiving feedback over the course of the study, the fingerprint quality of older participants improved significantly and at the end, prints of older women were of the best quality and also fewer attempts were needed to collect them.

Theofanos et al. (2007) conducted a study on how different instruction modes and an interaction with an operator influence the easiness of collecting ten fingerprints from users. They found that with operator assistance 98% of the participants were able to successfully provide their fingerprints. At the same time, only 56% of the participants who received poster instructions were successful. They also took longer than those receiving video or verbal instructions. The high success rate for participants receiving instructions from an operator shows that at least initially, users do require face-to-face guidance and it can be highly effective.

Nevertheless, both studies mentioned above were conducted on a subpopulation of knowledge workers who were highly computer-literate and motivated. The reality of where such a biometric reader would be deployed would be very different. As a usability person one has to also keep the worst case scenario in mind. In this situation, let us imagine an elderly person is waiting in a queue at an airport, the atmosphere is tense, they are under pressure to be quick to avoid embarrassment, they are unfamiliar with the technology, tired from the trip and overwhelmed. In this case, if something goes wrong, the user is "rejected by the system" or they need elaborate instruction to present their biometric feature they will feel *they failed* and not *the system failed*.

Although as the studies mentioned above show, training can be very successful, elaborate instruction and explanation how to use biometric systems should remain a secondary option. Striving for high system usability should be the solution. Being rejected by a piece of technology, ordered around or instructed is simply bad user experience and can be embarrassing or even humiliating. It gives users, elderly or not, the impression that there is something wrong with them and they do not conform to a "norm". The truth is the technology has its shortcomings, either the back-end has problems with identity verification or the user interface is unusable.

Careful design makes seniors more successful

In general, devices should be designed to optimise some capabilities while compensating for others (Hart et al., 2008). Elderly users are unlikely to develop a new mental model for that reason, newly created devices and systems need to fit into existing requirements, preferences and thought patterns (Holzinger et al., 2008).

Research has shown that pure compliance with guidelines is not sufficient. A study by Hart, Chaparro & Halcomb (2004, 2008) shows that sites designed with senior friendly guidelines in mind did result in higher task success but did not mean participants navigated through them quickly and efficiently. Compliance with these guidelines also did not result in higher user satisfaction or preference. For that reason, the researchers suggest using guidelines as a starting point and then combining them with usability testing to achieve a better result.

Practice improves performance

As mentioned earlier, some participants in the ATM study by Akatsu and Miki (2004) experienced a timeout and needed to start the operations from the beginning. Although this might have led to frustration, the time measurements show that the participants learned from their first unsuccessful attempt and were quicker at the second attempt. Also Ziefle and Bay (2006) found that older participants in their study performed distinctly better when completing the set tasks a second time. In comparison with the first run, their performance improved by an average of 6%. Their speed improved by 28%, it went from 14:26 in the first attempt to 10:17 in the second. The researchers also measured disorientation through returns in menu hierarchy and returns to the top. For hierarchical returns, there was a decrease from 33.1 to 28 (16%) in the two runs. For returns to the top, there was an improvement from 4.9 to 2.9 (41%) returns.

Exposure increases acceptance

Ideally, the more exposure and experience people have with computers, the more positive attitude they have. Coventry, De Angeli & Johnson (2003) describe that in a focus group prior to interaction with an ATM using iris verification, participants showed negative attitudes towards this technology. After interacting with the system, attitudes changed positively provided that the interaction was successful. The researchers suggest that there are several factors that could alleviate initial negative attitudes towards biometric technology, such as a marketing campaign, exposure to and experience with the technology. They suggest that enrolment could be a good opportunity to educate users.

However, Sasse (2007) stresses that there has to be consistency between the enrolment procedure and the subsequent use of the system. For example using the IRIS system at London Heathrow turned out to be confusing in this respect since the enrolment and subsequent use happen in two different environments. During the enrolment the individual sits down and the camera is adjusted to them, whereas during the actual use one is standing in front of a panel with three cameras and has to adjust to one of them. The adjustment is first downwards to bring one’s face into the field of view of the camera and second sideways to position one of the eyes in the target circles. Finally, one has to move forward or backward to be at the prescribed distance.

This “bendy shuffle” to make it possible for the limited technology to capture one’s biometric features illustrates a wider problem with biometric technologies. Namely, they assume the user would adjust themselves to the piece of equipment rather than the equipment would be adjusted to the user. And in the specific case of iris scanners, the pieces of technology that adjust themselves to the user, by being height adjustable and having autofocus, have been proven to perform significantly better (Secunet, 2005). Nevertheless, Coventry and Johnson (1999) stress that more adaptive biometric scanners come at a higher price and tend to take up more space. For that reason, purchasers are generally more reluctant to buy them.

4 Opportunities for biometrics

4.1 0-effort, 1-step, 2-Factor Authentication?

In a recent study funded by the US National Institute of Science and Technology (NIST), the authors detailed how the ever-increasing burden of knowledge-based authentication was damaging productivity and undermining security (Steves et al. 2013). The authors found many examples increasing 'friction' first identified by Beautement et al. (2008) because of increasing mental and physical workload associated with authentication. They were particularly incensed at the frequency with which they had to authenticate to the same systems and services over and over again – "*If I authenticated and did not move away from the computer, it should know that and not bother me again.*" Steves et al. also discovered that the disruptiveness of authentication on primary tasks meant several of their participants were frustrated by the "*insidious escalation of disruption over time on any one account or application."* Participants reported that they had opted out of using a number of technologies and services because of the disruptive nature of authentication. Considering the particular requirements of older users, disruption compounds the memory and concentration problems many users suffer from (see 3.1)

Steves et al. conclude that the time has come for a massive shift from these disruptive, explicit forms of authentication, to *implicit* forms of authentication, which recognise users without disrupting or bothering them, leveraging user interaction carried out as part of the primary task and the mode of interaction instead. Biometrics are the natural method of achieving this: users interacting with keyboards could be identified from their typing patterns (e.g., Maxion & Killourhy, 2010). Users of touchscreens on smartphones and tablets can be identified through their gestures or touch, whilst those using audio or video can be identified through voice or facial recognition. If combined with a knowledge based credential (a simple password they user types or speaks, or a shape entered on the screen, biometrics can provide a zero (or very low) effort, 1-step, 2-factor authentication. With this type of authentication, we can remove the barrier of secondary task authentication that older users otherwise struggle with.

But realising this vision requires increasing accuracy of performance of these biometrics, and predicting and futureproofing these biometrics against predictable ageing effects. Biometrics requiring constant re-enrolments would be as disruptive as passwords are today.

Briggs & Oliver (2009) have presented an intriguing idea of overcoming this problem: the *biometric daemon*. Inspired by the demons that every human character in Philip Pullman's Northern Lights is accompanied by, they propose a biometric device which is initially imprinted with the fixed biometric properties of its owner, and is then regularly updated with the fluid biometric properties of its owner. This would overcome the usability problems caused by current high false rejection rates. But what is particularly intriguing for older users is that they propose the demon could also acts as an electronic pet *"which (i) part-shares identity with its owner, (ii) needs nurturing and (iii) effectively dies when separated from its owner for any length of time."* Since the benefits of pet ownership and interaction on the physical and mental well-being of older adults are well-documented, the idea of a Tamagochi-type token being looked after by this user group, and offering friction-free authentication in return, is one worth exploring.

4.2 Replacing CAPTCHAs

In section 2.2, we discussed that security mechanisms that users cannot cope with can bar them from access to important services. One security mechanism that falls into this category are CAPTCHAs – *"Completely Automated Public Turing Test To Tell Computers and Humans Apart"* (Captcha, 2013). Service providers use this test to stop botnets from creating accounts which are then used for malicious purposes – such as sending spam, or in the case of a large European low-cost airline – to prevent screen-scraping of its prices by Web comparison sites. Whilst the security needs of the Websites are understandable, it makes all legitimate human users do extra work to access the sites. In a column in Scientific American published in February 2012, the technology writer David Pogue calculated that every day 17 man-years of effort are spent on decoding them (Pogue, 2012). In addition to increasing workload for some users – many of whom need 2-3 attempts to access a site – CAPTCHAs prevent a significant number of users, who struggle to decipher the squiggly warped letters, from accessing the site altogether (Bursztein et al., 2010) – and many of these are older users, among whom vision impairments are common (see 2.1). To improve accessibility for users who have problems with sight, audio CAPTCHAs like SoundsRight (Lazar et al., 2012) have been developed, but these do not necessarily offer an improvement for older users, and have also been shown to be easier to attack, provide a 'back door' for attackers as Bursztein & Bethard (2009) showed when they were able to overcome 75% of eBay's audio CAPTCHAs.

The usability problem with current CAPTCHAs presents an enormous opportunity for biometrics – proving that you are human using biometrics could be achieved in a low-effort, natural interaction. Since older users in particular struggle with CAPTCHAs, they would be chief beneficiaries – but as with the TV remote control (see 2.1) the increased convenience is likely to be welcome by all users.

5 Conclusions

As this chapter has shown, usability and security have not rubbed along well for quite some time, and users have paid the cost. If target users are not able to use the system correctly, it is not accessible – for the ageing population, the increasing workload and complexity of security solutions create the risk of exclusion.

In the context of security, accessibility is particularly important to consider for at least two reasons:

1) Many security mechanisms act as 'gatekeepers', providing access to systems or services. Thus, if the mechanism is not usable, it can undermine the accessibility not only of the gatekeeper but also of a wider range of systems.

2) When users find a system difficult or impossible to use, many of them will recruit help from others: friends, family, or employees of a service provider, for instance. The vast majority of helpers will be trustworthy, well-intended, and act in the users' best interest, but the suggested assistance of others often undermines the assumptions made by the designers of the security mechanisms, and security itself.

As discussed in the previous section, the increasing use of devices and services that require authentication by all segments of the population, including the ageing population. All services – including government ones – now expect users to trust online. The low usability of existing knowledge-based authentication mechanisms has led to authentication fatigue and habitual casual circumvention of security mechanisms. There is now widespread recognition that purely knowledge-based authentication is not secure: with cloud computing, passwords can be cracked in increasingly short time – and length and complexity of passwords required to withstand such attacks makes them unusable (Arnell et al., 2012). Add to this the proliferation of consumer-owned devices which are impossible to secure (unless Trusted Computing suddenly is adopted widely), and the need for 2-factor authentication become obvious.

Most current 2-factor solutions are token-based, and anything but usable: most involve at least 3 steps as well as 2 factors, the user has to remember to carry the device – something that older people may find problematic.

This current state of affairs presents a significant opportunity for biometrics to come to the rescue, and offer convenient solutions that minimise user workload and create minimal disruption to their primary tasks. But in addition to meeting the specific characteristics of the ageing user population, solutions must also fit into the tasks and contexts in which these users operate. That fit means we want biometric to 'disappear' into users tasks – which suggests a range of different biometrics embedded in devices and services.

This suggests a large infrastructure project, which needs to be tackled sooner rather than later. The UK government's approach to joint public and private sector, using federated identity (Government Digital Service, 2013) mentions that authentication must be accessible as well as secure, but it has not specified specific usability criteria, and makes no specific mention of biometrics. In our view, this is a mistake, since it a significant infrastructure project will be required to deliver usable and secure authentication for all sections of the population, and it requires policy, not just technology:

As Challenger and Clegg (2001) pointed out:
"When designing and operating any new system it is critical to focus on and optimise both technical and social factors (e.g. Cherns, 1976, 1987). It is inevitable that

changes to one part of a system will necessitate subsequent changes to other parts; thereby, to optimise success, the system should be considered holistically (e.g. Hendrick, 1997; Clegg & Shepherd, 2007). Thus, people, processes and procedures, goals, culture, technology, and buildings and infrastructure should all be viewed as interdependent and given joint consideration."

It is hard to imagine that individual service providers will take this perspective. There must be a concrete set of information about the users and their goals and tasks that the design can be fitted to – defining a usable mechanism without first defining the system it is to be used in can only result in wasted effort.

References

A. Adams & M.A. Sasse (1999): 'Users are not the enemy: Why users compromise security mechanisms and how to take remedial measures'. Communications of the ACM, 42(12), 40–46.

H. Akatsu & H. Miki (2004): 'Usability research for the elderly people'. Oki Technical Review (Special Issue on Human Friendly Technologies); 71(3), 54–57.

S. Arnell, A. Beautement, P. Inglesant, B. Monahan, D. Pym & M.A. Sasse (2012): 'Systematic decision making in security management modelling password usage and support'. Proceedings of the International Workshop on Quantitative Aspects in Security Assurance (QASA 2012). Pisa, Italy.

A. Beautement, M.A. Sasse & M. Wonham (2008): 'The compliance budget: Managing security behaviour in organisations'. Proceedings of the 2008 Workshop on New Security Paradigms. ACM, Lake Tahoe, CA. pp. 47–58.

J. Botwinick (1984): Aging and Behavior: A Comprehensive Integration of Research Findings (2nd edn.). New York, NY: Springer.

P. Briggs & P.L. Olivier (2008): 'Biometric daemons: authentication via electronic pets'. CHI'08 extended abstracts on Human Factors in Computing Systems. Florence, Italy. ACM, pp. 2423–2432.

S. Brostoff & M.A. Sasse (2000): 'Are passfaces more usable than passwords? A field trial investigation'. People and Computers XIV-Usability or Else!, 405–424, Springer London.

E. Bursztein, S. Bethard, C. Fabry, J.C. Mitchell & D. Jurafsky (2010): 'How good are humans at solving CAPTCHAs? A large scale evaluation'. 2010 IEEE Symposium on Security and Privacy (SP). IEEE. pp. 399–413.

E. Bursztein & S. Bethard (2009): Decaptcha: Breaking 75% of eBay audio CAPTCHAs. Proceedings of the 3rd USENIX Conference on Offensive Technologies. USENIX Association, p. 8.

V. Cantin, M. Lavallière, M. Simoneau & N. Teasdale (2009): 'Mental workload when driving in a simulator: Effects of age and driving complexity'. Accident Analysis & Prevention, 41(4), 763–771.

A. Calero-Valdez, M. Ziefle, F. Alagöz & A. Holzinger (2010): 'Mental models of menu structures in diabetes assistants'. In: K. Miesenberger, J. Klaus, W. Zagler & A. Karshmer (Eds.), ICCHP 2010. LNCS, vol. 6180, pp. 584–591.

CAPTCHA (2013): http://www.captcha.net/

R. Challenger & C.W. Clegg (2011): 'Crowd disasters: A socio-technical systems perspective'. Contemporary Social Science, 6(3), 343–360.

L. Coventry & G.I. Johnson (1999): 'More than meets the eye! Usability and iris verification at the ATM interface'. In: S. Brewster, A. Cawsey & G. Cockton (Eds.), Human-Computer Interaction: Interact 99, IOS Press/IFIP, pp. 151–156.

L.M. Coventry, A. De Angeli & G. Johnson (2003): 'Usability and biometric verification at the ATM interface'. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, pp. 153–160.

S.J. Czaja & J. Sharit (1998): 'Age differences in attitudes toward computers'. Journal of Gerontology, 53B(5), 329–340.

S.G. Davies (1994): 'Touching Big Brother: How biometric technology will fuse flesh and machine', Information Technology & People, 7(4), 38–47.

R.D. Ellis & J.C. Allaire (1999): 'Modeling computer interest in older adults: The role of age, education, computer knowledge, and computer anxiety'. Human Factors, 41(3), 345–356.

D. Gentner & A.L. Stevens (1983): Mental Models. Hillsdale: L. Erlbaum.

Government Digital Service (2013): 'ID assurance', http://digital.cabinetoffice.gov.uk/category/id-assurance/

L. Groff, C. Liao, B. Chaparro & A. Chaparro (1999): 'Exploring how the elderly use the web'. Usability News, 1(2), 1–2.

T.A. Hart, B.S. Chaparro & C.G. Halcomb (2004): 'Designing websites for older adults: The relationship between guideline compliance and usability'. Proceedings of the Human Factors and Ergonomics Society Annual Meeting (vol. 48, no. 2, pp. 271–274). Sage New Orleans, Louisiana.

T.A. Hart, B.S. Chaparro & C.G. Halcomb (2008): 'Evaluating websites for older adults: Adherence to 'senior-friendly' guidelines and end-user performance'. *Behaviour & Information Technology,* 27(3), 191–199.

L. Hasher, R.T. Zacks & C.P. May (1999): 'Inhibitory control, circadian arousal, and age'. In: D. Gopher & A. Koriat (Eds.), *Attention and Performance XVII: Cognitive Regulation of Performance. Interaction of Theory and Application* (pp. 653–675). Cambridge, MA: MIT Press.

T. Hedden & J.D.E. Gabrieli (2004): 'Insights into the ageing mind: A view from cognitive neuroscience'. *Nature Reviews Neuroscience,* 5, 7–96.

C. Herley (2009): 'So long, and no thanks for the externalities: The rational rejection of security advice by users. *New Security Paradigms Workshop (NSPW).* Oxford, UK.

R.J. Hodes & D.A.B. Lindberg (2002): 'Making your website senior friendly'.

http://www.nlm.nih.gov/pubs/checklist.pdf

A. Holzinger, G. Searle, T. Kleinberger, A. Seffah & H. Javahery (2008): 'Investigating usability metrics for the design and development of applications for the elderly, In: K. Miesenberger, J. Klaus, W.L. Zagler, A.I. Karshmer (Eds.), *ICCHP 2008,* Springer, Berlin Heidelberg.

P.G. Inglesant & M.A. Sasse (2010): 'The true cost of unusable password policies: Password use in the wild, *Proceedings of the 28th International Conference on Human Factors in Computing Systems (CHI'10)*. Atlanta, USA. pp. 383–392.

International Organization for Standardization (ISO) (2010): ISO 9241-210: 'Ergonomics of human-system interaction—part 210: Human-centred design for interactive systems, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52075

P.M. Johnson-Laird (1983): *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness*. Harvard University Press, Harvard.

M.K. Johnson, J.A. Reeder, C.L. Raye & K.J. Mitchell (2002): 'Second thoughts versus second looks: An age-related deficit in reflectively refreshing justactive information'. *Psychological Science*, 13, 64–67.

J. Lazar, J. Feng, T.Brooks, G.Melamed, B.Wentz, J.Holman, . . .& N. Ekedebe (2012): 'The SoundsRight CAPTCHA: An improved approach to audio human interaction proofs for blind users'. *Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems*. Austin, TX. ACM, pp. 2267–2276.

H. Makishita, & K. Matsunaga (2008): 'Differences of drivers' reaction times according to age and mental workload'. *Accident Analysis & Prevention*, 40(2), 567–575.

R.A. Maxion & K.S. Killourhy (2010): 'Keystroke biometrics with number-pad input'. In *IEEE/IFIP International Conference on Dependable Systems & Networks* (DSN-10, Chicago, IL. IEEE Computer Society Press, Los Alamitos, CA. pp. 201–210).

A.S. Melenhorst, W.A. Rogers & E.C. Caylor (2001): 'The use of communication technologies by older adults: exploring the benefits from the user's perspective'. *Proceedings of the Human Factors and Ergonomics Society 45th Annual Meeting*. Human Factors and Ergonomics Society, Santa Monica, CA.

M. Obrist, R. Bernhaupt, E. Beck&M. Tscheligi (2007): 'Focusing on elderly: An iTV usability evaluation study with eye-tracking. In: P. Cesar, K. Chorianopoulos, and J.F. Jensen (Eds.), 5th European Conference on Interactive TV – EuroITV 2007 May 24, 25, 2007, Amsterdam, The Netherlands, pp. 66–75.

D. Pogue (2012): 'Time to kill off CAPTCHAs', *Scientific American*, http://www.scientificamerican.com/article.cfm?id=time-to-kill-off-captchas

W.A. Rogers (2000): 'Attention and ageing', In: D.C. Park and N. Schwarz (Eds.), *Cognitive Aging: A Primer* (pp. 57–73). New York, NY: Psychology Press.

M.A. Sasse (2007): 'Red-eye blink, bendy shuffle, and the yuck factor: A user experience of biometric airport systems'. *IEEE Security&Privacy*, 5(3), 78–81.

D.E.A. Sayago (2006): 'Some aspects of ICT accessibility, usability and design methods with the young elderly', http://www.dtic.upf.edu/~ssayag/dea_sayago_July06.pdf

Secunet (2005): 'Untersuchung der Leistungsfa¨higkeit von Biometrischen Informationssystemen—BioPII' (A study of the performance of biometric systems), Öffentlicher Abschlussbericht, https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/biop/BioPII.html

M. Steves, D. Chisnell, M.A. Sasse, K. Krol & H. Wald (2013): *Report: Authentication Diary Study*, National Institute of Standards and Technology, Gaithersburg, MD, USA.

J.M. Tanner (1989): *Foetus into Man: Physical Growth from Conception to Maturity*. 2nd edn. Castlemead, Ware.

M. Theofanos, R. Micheals, J. Scholtz, E. Morse & P. May (2006): 'Does habituation affect fingerprint quality?' *Proceedings of the 24th International Conference on Human Factors in Computing Systems (CHI'06)*. Montre´al, Canada.

M. Theofanos, B. Stanton, S. Orandi, R. Micheals & N.F. Zhang (2007): 'Ten-print fingerprint capture: Effect of instructional modes on user performance'. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (vol. 51, no. 10, pp. 597–601). Sage. New Orleans, Louisiana.

M.I. Worcester, A. Loustau & K. O’Connor (1990): ‘Tailoring teaching to the elderly in home care’, *Home Health Care Services Quarterly*, 11(1–2), 69–120.

M. Ziefle & S. Bay (2006): ‘How to overcome disorientation in mobile phone menus: A comparison of two different types of navigation aids’. *Human Computer Interaction*, 21(4), 393–432.