

Now What Was That Password Again?

A More Flexible Way of Identifying and Authenticating our Seniors

Karen Renaud and Judith Ramsay
University of Glasgow & University of Paisley
karen@dcs.gla.ac.uk

The Web offers facilities which can make a huge difference to the lives of users with reduced mobility, something that affects many older users. Users have to be authorised to access restricted websites. This involves a two-step process: identification and authentication. These issues have received scant attention when considering the needs of specific user groups. Web identification and authentication is often treated as a one-size-fits-all problem with ubiquitous use of the password as an authenticator and a variety of different identification mechanisms being used. Neither is tailored to the needs of either the website or the target users. This paper discusses problems related to identification and authentication of older web users, and reports on experiences with field tests of initial solutions.

1 Introduction

Increasing the use of the web is not merely something that should be encouraged because it is such a valuable source of information. Populations throughout the first world are ageing (Engardio & Matlack 2005). This potentially means a larger number of people with limited mobility, increased isolation (Goodman, Brewster & Gray 2004), consequent loneliness (Cattan, White, Bond & Learmouth 2005) and depression (Dening & Barapatre 2004). This can be alleviated by the web because of the ease with which it facilitates worldwide, near-instant communication and home-based purchasing. This is not merely speculation. Studies by the Pew Internet and American Life Project (Fox 2001) have found that although fewer American older users are connected to the internet than younger users, they are nevertheless very enthusiastic users, an enthusiasm that has been confirmed in other studies, such as (McMellon & Schiffman 2002). The most widely used application, unsurprisingly, is email. Fox (Fox 2001) found that older users became more adventurous in their use of the web over time and usually used it for at least two years before purchasing anything on the web.

To encourage increased web usage we should therefore identify the barriers to its wide-spread uptake so that they can be addressed. One problem for web users of all ages is the issue of security (DTI 2005, Deloitte 2005). Whereas anonymous browsing holds few risks, communication- and retail-oriented web usage requires websites to ensure that only legitimate users gain access. This helps maintain the three goals of information security: confidentiality, integrity and availability (Pfleeger & Pfleeger 2003). Most information systems prevent illicit access by using site-specific user identities and passwords. This mechanism does not, unfortunately, accommodate the needs of anything other than a homogeneous group of users with perfect recall, dexterity and technical ability.

Much attention has been paid to designing web sites for the aged (Hawthorn 2003, NIA & NLM 2002, Becker 2004, W3 1999), but one of the biggest obstacles still remaining is the issue of both identification and authentication of users (Rash 2002), which generally requires 100% correct recall and error-free entry of a sequence of characters and numbers, a procedure that becomes increasingly error-prone with age or illnesses that impact on memory.

In order to accommodate *all* possible users of a system, it is important to consider the particular needs of the target user groups being served by a particular website in choosing the identification and authentication mechanism to be used. User groups consist of people with varying capabilities and these need to be catalogued carefully before the mechanisms are chosen so that they can be given serious consideration.

It is also necessary to consider site content. If this is done the security maintained by the mechanism can be tailored to the needs of the site in the same way as door locks of different strengths are chosen to protect different kinds of buildings. For example, passwords have the potential to be a very strong authentication mechanism — with an unlimited number of possibilities. In reality people usually make use of a word in their own language: limiting the possibilities to 10^6 in a language like English. Since most websites have a policy of 3-tries-lockout these odds are probably large enough to protect most web content. However, in some cases, the password is too strong to protect fairly innocuous web content. Maintaining security is not a simple one-size-fits-all problem. Developers should consider using purpose-tailored identification and authentication mechanisms, both in terms of site content and target user group.

In Section 2 the needs of older web users are considered. In Section 3 the idea of using handwriting recognition as a cue during authentication is discussed, and the particular problems related to identification and authentication for this particular user group are explored. Section 4 gives the details of a website which uses specially tailored identification

and authentication mechanisms. The identification mechanism is more flexible than usual identification schemes and the authentication mechanism is based on recognition rather than recall. Both mechanisms have been evaluated and the results of the evaluation are given. Section 5 concludes.

2 Older Users

In 1997 Stewart stated that the needs of older users were seldom accommodated by system designers (Stewart 1997). Nine years later not much has changed. Sites still expect users to remember many different passwords for sites used infrequently and issue users with password guidelines that are almost impossible to obey if the password is to be retained. For example, many sites ask users to define a password that contains both upper and lower case letters, include a numeral and a special character. While these guidelines are defined to make it harder for intruders to guess the password, it also makes such passwords almost impossible to remember without a physical record.

In order to accommodate user needs we should first consider the characteristics of this group of users. It should be borne in mind that older users are not a homogeneous group. Indeed, Maddox and Douglas (Maddox & Douglas 1974) argue that this group is actually more heterogeneous than younger groups of people.

It is an inescapable fact that people change as they age (Craik & Bialystok 2006). Some of the changes are in the area of notable changes in cognitive and perceptual performance. For example, elderly people, in particular, find it challenging to retrieve names and terminology (Cohen & Burke 1993).

The ageing brain should not merely be thought of as being characterised by diminishing abilities but rather by increasing sophistication. Elkonon Goldberg (Goldberg 2005) calls this phenomenon the *wisdom paradox* — arguing that whereas young brains are well suited to problem solving and have excellent short-term memory, older brains are much better at what he calls *pattern matching*. The older brain has accumulated much experience over the years and is extremely proficient at matching new situations to older ones and solving problems in that way. Hence the older brain has wisdom and the younger brain raw processing power. This means that cognitive ageing is *not* simply development in reverse. Hence cognitive changes that come with age are not so much due to the waning of mental ability, but rather due to individuals using different parts of the brain to less advantageous effect, for the same tasks (Logan, Sanders, Snyder, Morris & Buckner 2005).

Other positive changes are also evident. Mather and Carstensen (Mather & Carstensen 2005) saw that as the age of an individual increases, more positive than negative affect (emotion) is recounted. Pennebaker and Stone (Pennebaker & Stone 2003) (p291) observe that *with increasing age, individuals use more positive and fewer negative affect words, use fewer self-references, use more future-tense and fewer past-tense verbs, and demonstrate a general pattern of increasing cognitive complexity*.

Unfortunately the older computer users of the early 21st century have been catapulted into a technology-obsessed world where they don't have the internal patterns which would help them to deal with computer-related situations in the way they would deal with other situations — by matching them to previous patterns. Hence they have to deal with new situations using a younger person's strategies, and in applying this strategy they have face challenges in one or more of the following areas:

- *Cognition:*

- *Learning:* The Internet is new to everyone, but for older people learning how to use websites is an even bigger challenge because it is harder to learn as one ages (Botwinick 1967). The *ability* to learn is not impaired but the *rate* of learning is reduced (Salthouse 1985). This is not helped by the fact that older people seem to believe that they are too old to learn (Timmerman 1998, Roberts 2001). There is some evidence that the use of computers can actually assist in this process (Shapiro 1995) and older computer users appear to actively pursue learning (Kiel 2005). Their motivation for this is that some of them appear to believe computers make life easier [ibid] and that using computers can reduce mental decline. Older people master new skills differently (Lindeman 1947), utilising experience more than younger people so that training programs and documentation targeted to the needs of younger people will not necessarily meet the needs of older computer users.
- *Attention:* Any use of a computer interface requires the ability to focus attention for a period of time so that a deficiency in this area can be very disabling. Unfortunately, the ability to pay attention diminishes with age (Stankov 1988). Hawthorn (Hawthorn 2000) distinguishes between *selective* and *divided* attention and examines the evidence of maintenance of these in older people. The former is the kind of attention needed to focus on a particular piece of information and to filter extraneous detail out. He cites research that shows that this ability deteriorates with age.

Divided attention, on the other hand, requires users to pay attention to more than one thing at the same time. The ability to divide one's attention depends upon the degree of challenge set by the task, the individual's experience and the similarity of the tasks themselves (Treisman & Davies 1976).

Hawthorn [ibid] points out that there is less agreement about the effect of age on this ability — he explains that some researchers report observing a decline in this ability with age while others have found that this only

occurs when users are dealing with complex tasks. It is clear from Hawthorn's discussion, however, that when complex tasks are involved older users find it harder to multi-task.

- *Memory*: Older people often develop short-term memory limitations (Akatsu & Miki 2004). This problem needs to be given serious consideration by not requiring users to remember nonsensical and unrelated facts such as numbers of passwords and/or user names. Since everyone, regardless of age, finds it easier to recognise than to recall (Merriam & Cunningham 1990), this ability should be exploited.
- *Dexterity* – Older users often have problems using the mouse and keyboard (Czaja 1996). They sometimes struggle to click on small targets and even double-clicking becomes difficult as reaction times slow (Chadwick-Dias, McNulty & Tullis 2003). These coordination problems are caused by tremors or arthritis so web sites should not require users to point too precisely with the mouse or to type a long character strings without errors (Chisnell & Redish 2005), especially when keys repeat due to delayed reactions (Kelley & Charness 1995).
- *Vision*:
 - *Print size* — Older users may have failing vision which means that they should not be required to observe very fine details on the screen (Chisnell & Redish 2005). They like large print and less content on pages (Chisnell, Lee & Redish 2004) and pages should not be too busy because they also have reduced visual processing speed (Jackson & Owsley 2003).
 - *Colour* — age affects colour discriminating ability. There is evidence that eye lenses yellow with age (Pokomy, Smith & Lutze 1987). Since yellow is often used to attract attention colours should be used carefully and with some understanding of age differences in colour vision.
- *Hearing*: Many older users are hard of hearing and this can increase their sense of loneliness and affect their self-esteem negatively (Chen 1994). In terms of web usage we should ensure that any information which is transmitted audibly is also provided in another format so that hearing-impaired users don't miss out on important information.
- *Time*: Older users tend to be less impatient (Trostel & Taylor 2001) and do not want to be hurried (Chisnell et al. 2004), probably because they do things more slowly (Mazaux, Dartigues, Letenneur, Darriet, Wiart, Gagnon, Commenges & Boller 1995). Thus the time-consuming nature of various activities is less of an issue in systems developed for older users. This is an important finding. Much effort goes into ensuring that web users get a response within particular limited time boundaries because it is well known that web users have low tolerance for waiting (van Iwaarden & van der Wiele 2003). This is a very restrictive constraint that is removed when catering for older users.
- *Special Requirements*: Some older users have a limited understanding of computers and the Web and any special software or hardware that needs to be installed, or technical expertise required, could be a barrier to the use of the Web site.
- *Psychosocial Factors*: Many older users become depressed due to their increasing isolation, loneliness and ill health (McCrae, Murray, Banerjee, Huxley, Bhugra, Tylee & Macdonald 2005). There is some evidence that older people can use computers to combat loneliness (Clark 2002), but there is no evidence of wide-spread use of e-commerce as yet, even though many businesses are well aware of the potential spending power of what they call the "gray market" (Brennan 1997). There is also evidence that increased use of computers will reduce negativity and a feeling of being sidelined by technology (Morris 1994).

Older people often experience anxiety and, more specifically, computer-related anxiety appears to increase with age (Laguna & Babcock 1997). This is something that is exacerbated by the use of jargon and ill-formulated error messages. However, if they are able to master the skills required to use the Internet and email, the accompanying feeling of competence could well improve their feeling of well-being, an effect that Ranzijn *et al.* found in their study of self-esteem in elderly adults (Ranzijn, Keeves, Luszcz & Feather 1998).

Chisnell and Redish (Chisnell & Redish 2005) also refer to the need to consider *attitude*. This refers to the confidence levels of the user. They point out that some older users are more likely to take risks and to experiment than others, and that this can help in introducing them to the web.

Many older people spend much of their time paying visits to friends and relatives, watching television, reading or gardening. These activities meet older people's needs such as socialising, self-fulfilment, closeness to nature, exercise, and learning (McAvoy 1979). There is great potential for the Internet to support these users in meeting at least some of these needs.

Maintaining accessibility in order to accommodate such a range of abilities is challenging. This paper will look at only one area — giving due consideration to this target group in choosing the identification and authentication mechanism.

This section discussed the particular challenges in developing systems for older users. It is very difficult, if not impossible, to address all of them. There are some that can be catered for with a little serious effort. For example, one can

avoid using sound cues if users with hearing loss are expected. One can also easily facilitate larger fonts and tailorable colour schemes.

Other challenges are much harder to cater for. One example is dexterity. If users have problems using the keyboard then one has to allow mouse-only input and if they have problems using a mouse efficiently one needs to facilitate keyboard entry. Many older users have arthritis, which makes both keyboarding *and* mouse usage difficult. The best one can do in this situation is to design the website so that it does not impose rigid time constraints on users and supports their text entry with a spell checker so that errors need not be disastrous.

3 Meeting Challenges

In a world where access to digital spaces is mostly achieved by means of a shared secret, a short-term memory problem is challenging. A serious alternative to passwords is a graphical authentication mechanism that relies on the user's own recognition process rather than perfect recall. This kind of authentication can be performed using a standard browser, which eliminates the need for additional equipment. These systems have a superior solution to memorability problems, compared to entering alphanumerical passwords, since people have an innate ability to remember pictures better than words (De Angeli, Coutts, Coventry & Johnson 2002). De Angeli *et al.* categorised such systems based on the actions required of the user during authentication. One of the categories is the recognition-based mechanism, also called *cognitive* authentication (De Angeli, Coventry, Johnson & Renaud 2005). This requires the user to recognise and identify target images from a set of displayed images. The displayed images could be photos of faces (Brostoff & Sasse 2000), representational objects such as those used by VIP (De Angeli *et al.* 2002) or abstract pictures such as the ones used by Dèjà Vu (Dhamija & Perrig 2000).

Although graphical recognition-based mechanisms support access codes that are more memorable than those supported by recall-based mechanisms, they offer no other cues to the forgetful user. The provision of cues is always a tricky issue, since cues need to be helpful to the legitimate user but not to the intruder. One therefore has to provide cues that will make sense only to the legitimate user. Weinshall (Weinshall 2004) proposes an ingenious scheme whereby a cue is provided by a slight change in the image being displayed which the user has been trained to observe. The theory is that an imposter's change-blindness (Rensink 2002) will prevent him or her from seeing the slight changes and thus the cue will only be observed by the legitimate user. Unfortunately the changes to the images have to be fairly slight in order to go unobserved by an impostor and thus this scheme will not work very well for users with failing sight or attentional difficulties.

Another way to supply cues within an image is to use non-representational images based on a biometric such as the user's handwriting. Back in 1895, Preyer found that a person would produce the same handwriting using either of their hands or feet and proved that handwriting was not determined by the appendage used to produce it but rather by some other process in the brain. He called handwriting "brainwriting" since it was created automatically and impulsively, without any conscious thought or awareness of the formation of the letters or numerals. In more recent publications Longcamp *et al.* (Longcamp, Anton, Roth & Velay 2003) argues that individuals recognise their own handwriting not just visually but also because it is related to the learnt process of writing the letters and numerals, something referred to as "kinaesthetic facilitation" (Seki, Yajima & Sugishita 1995), which is combined with the visual control process (Zimmer 1982). A direct consequence of this is that people recognise their own handwriting, even many years after they have produced it.

Handwriting recognition is a skill that is completely effortless and, like many other implicitly learnt skills, it does not degrade with age or time. Heckman *et al.* (Heckman, Lang & Neundorfer 2001) carried out experiments with stroke and dementia patients and concluded that handwriting recognition was a special skill which was independent of verbal and lexical tasks. Srihari *et al.* (Srihari, Cha, Arora & Lee 2001) found that in 98% of 1000 cases, the handwriting was clearly individual and this makes it particularly suitable for use by a recognition-based authentication scheme. Furthermore, most importantly in terms of our proposed use of this skill during authentication, is that people cannot formulate the way they do this — the knowledge is tacit, not factual, and this reduces the potential for transfer of the knowledge to an intruder.

Handwritten signatures have been used to authenticate humans for many years, and some shops are still accepting this form of authentication when customers pay for purchases with a bank card. A signature can, however, easily be recognised by people other than the signature owner, and something less universally-recognisable is needed in order for images of the user's handwriting to be used in online authentication. Srihari *et al.* (Srihari *et al.* 2001) determined that words had more individuality (more difference) than alphanumerical characters, and that characters had more individuality than numerals. Individuality, in this sense, refers to traits which make it possible to identify the author of a handwriting sample. It is harder for another person to deduce the authorship of a numeral sample than of a letter or word sample. Due to the inherent human handwriting recognition ability, and the need to make the system as secure as possible, the use of numerals in recognition-based authentication is the only viable option. The cue the image provides is of limited use to intruders while still providing a meaningful and helpful cue to the legitimate user.

A biometric which is not as popular as handwriting is line drawings or doodles. This is something which even family members of the user may not easily recognise. However, it, too, provides cues to the legitimate user, related to the contribution of the user's previous action-planning structures which support recognition (Knoblich & Prinz 2001). The

level of cues provided by handwriting disqualifies their use in systems requiring strong authentication. However, their use for a low-risk website is justified by the increased memorability. The following sections will discuss the particular problems presented by identification and authentication in a web context.

3.1 Identification

Web users are basically identified in one of two ways — by what they hold (a smart card) or by what they know. Smart cards work admirably and can be tailored for the use of older users (Gill 2004), but they can also be mislaid (something that plagues older users) or stolen. They are currently fairly costly to issue so their use will probably be restricted to high risk sites. Hence this stage probably depends on the ability to type a fairly long string of letters and numbers correctly. This is by no means an infallible skill — individuals who have dyslexia have problems with this, as do individuals with dyspraxia and arthritis, not to mention skills more attuned to manual typewriters.

Identification, at first sight, does not have to be as secure as authentication, since the authentication stage secures the system. However, when one reads hackers' accounts of successful sensitive system break-ins it becomes clear that the first step is obtaining a valid login name, and only once that has been obtained can the authentication key be broken. Hence it may not be wise simply to display a list of user names for the curious outsider to use. On some systems, such as eBay, user names are available for anyone to see. This choice is obviously made because eBay users have to be able to contact each other and explore seller and buyer integrity by means of feedback ratings. However, eBay sometimes suffers from fraudulent activities (Cox 2002) and it could well be facilitated by the visibility of user names. It is necessary to tailor the visibility of user names to the needs of the website but also to consider security and privacy requirements. Developers have some choices to identify web users:

- *automatically*
 - Use a cookie¹. This is quite effective on dedicated personal computers, but not for users of shared computers. Furthermore, many users either delete cookies regularly or do not permit them due to the unwelcome presence of spyware, which is facilitated by cookies.
- *recall-based*
 - Use a special site-specific user name. This is sometimes not a good solution since the user now has an additional memory burden. She not only has to remember a password but also a unique user name.
 - Use the user's email address. This only works for users with dedicated email addresses. Another disadvantage is the universal visibility of email addresses. Furthermore, if users are required to identify themselves by means of an email address they have to type it in correctly every time — and email addresses are fairly long strings.
- *recognition-based*
 - Provide a list of user names and allow the user to click on one. Unfortunately this is too insecure for most sites requiring authentication since it gives the hacker the first half of what she requires to enter the site. Even if this mechanism *is* acceptable in terms of security, it is still a problem in terms of privacy since users, for whatever reasons, may not wish to advertise their membership and use of a particular website.

In terms of memory load the best option appears to be the use of an email address, which the user already knows, so it does not place an extra memory burden on him/her. However, it is necessary to investigate the usability of this. The website using the Handwing (Renaud 2005) authentication mechanism requires users to identify themselves by means of their email address. As time elapsed it became clear that the email-oriented identification was less than satisfactory. Many of the users shared email addresses. This served their purpose and they did not see the need to maintain another email address so email addresses could not be used to identify users uniquely.

Furthermore, users made many errors in entering their email addresses. Over a 50 day period during which the failed identifiers were recorded there were 42 reports. If one considers an email address to take the format: prefix@subdomain.domain.country, the problems experienced can be classified into one of the following:

1. Only the email address prefix entered (11)
2. Extra character inserted or character left out, or incorrect character used (such as > instead of .) (23)
3. Incorrect email address (5)
4. Rubbish (3)

¹A cookie is a file that is stored on the user's machine which the web browser uses to identify the user at subsequent visits to the same site.

In order to address these problems the site was altered so that users could define a unique user name which they could use to log into the site instead of their email address. Disappointingly, few users chose to define such a user name and the new facility remained largely unused, with the exception of one user with a particularly long email address, similar to dannyandjane@somewhere.co.uk. This user was responsible for many of the identification errors and as soon as she switched the errors ceased. Users were also allowed to use only the email address prefix to identify themselves. This accommodates users falling into the first category because for a site with only 60 users all email prefixes are unique. It also addresses the problems in category two since such errors are more likely the longer the email address.

Thus the remaining problem to be dealt with was that users needed to identify themselves in spite of typing difficulties and resulting errors. On the other hand it was not possible to display a list of user names because that would impact on user privacy. Users needed to demonstrate that they had a knowledge of their user name even if they were unable to type it correctly. The typing difficulty experienced by users using their email addresses was dealt with by identifying users with the following simple algorithm (as illustrated in Figure 1):

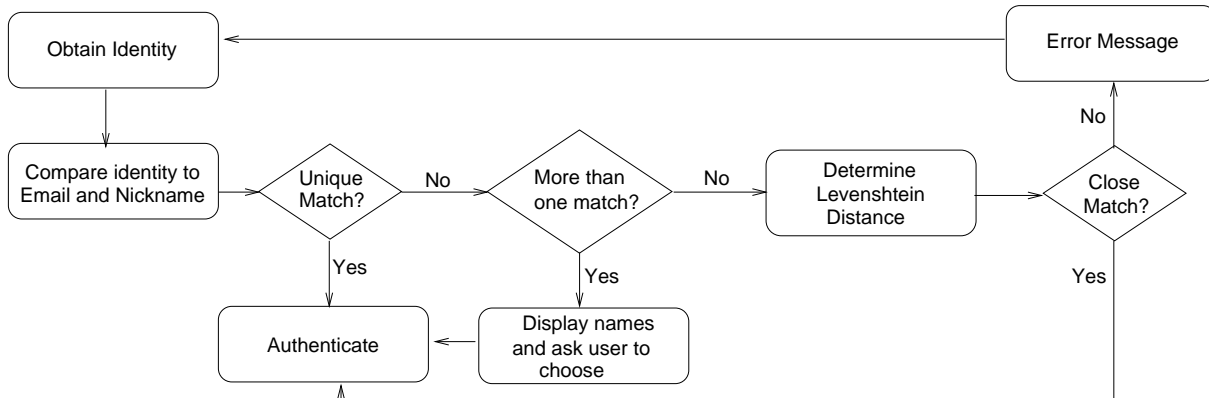


Figure 1: Identification Algorithm

1. Verify the identification string.
2. If it is uniquely identifiable, proceed to authentication.
3. If it matches more than one user’s email address, display the names of the people registered with that email address and ask the person which one he/she is (This accommodates shared email addresses). Authentication follows.
4. If it does not match any of the email addresses, proceed to an approximation process.

The process works out the similarity between the entered email address and the email addresses of registered users. There are two well-established ways of doing this: equivalence methods and similarity ranking. The latter is suitable for this application since it is necessary to determine the distance between what the user has entered and any of the legitimate addresses to accommodate errors. Levenshtein distances (Levenshtein 1965) are calculated to measure the similarity of two strings in terms of a *distance*. The distance indicates the number of deletions, insertions and substitutions needed to transform the given email address to any of the users’ email addresses. This quantifies the difference between the two email addresses that can be used to support decisions about whether to accept the similarity as being due to error or whether the attempt should be denied.

It is necessary to set a cutoff point — setting the permissible distance (number of permissible errors). This allows us to distinguish between genuine errors and hacking attempts. One can set either a percentage difference or a specific number of incorrect characters that will be tolerated:

- (a) Upon examining all errors made during the monitoring period it was concluded that a Levenshtein distance of 3 would sufficient relax the rigidity of the identification process — thus there could be 3 incorrect or missing characters in the identification string.
- (b) The other option is to use a similarity percentage of 90%. However, whereas a Levenshtein distance of 3 denotes a very similar string, just one character difference in a short email address could deliver a much smaller similarity percentage. Thus even though the distance is acceptably small in number terms the similarity percentage is unacceptably large.

A decision was therefore made to allow a Levenshtein distance of 3 characters *or* a similarity percentage of 90% would be tolerated. All identification attempts were logged in order to monitor algorithm performance.

Section 4.1 reports on the evaluation of the mechanism.

3.2 Authentication

Since biometrics' special hardware or software requirements mostly disqualify them for web usage, Web users are usually authenticated by means of either a password on its own or accompanied by a token such as a smart card. Passwords are used by system developers under the mistaken impression that they are a quick and easy way of authenticating users and indeed for the developer this is true. However, in considering the two other groups of people affected by this decision during the lifetime of the system — end users and system administrators — it is clear that it is neither quick nor easy.

Passwords get forgotten and have to be replaced, they are stolen, guessed and broken by persons of ill intent. System administrators have no reason to whole-heartedly approve of passwords either. Reports of between a third (Walker 2001) and a half (Doran 1999) of help-desk calls being related to passwords emphasise the size of this problem. Gartner published a report in 2004 claiming that it costs \$15-30 to change a password for a 2,500 person firm and that, on average, each employee will call four to five times per year (Witty & Brittain 2004). Hence it is not merely arduous or annoying to handle this problem but also expensive.

Whereas it is possible to be quite relaxed about identification, as discussed in the previous section, there is no such leeway when it comes to authentication. One cannot accept a mere approximation of the authentication key — it has to be identical to the stored key. In order to support older users during authentication, it is necessary to match the skills required to authenticate correctly with the skills that generally do not decline with age and thus to accommodate the specific problems that many older users have. The authentication step should specifically accommodate the following, as discussed in Section 2, and contrasted with traditional passwords:

1. *Memory* — one should rely on recognition and not on faultless recall, which is the main problem with passwords.
2. *Hearing* — one should not utilise any sounds to communicate either errors or success that is not also communicated in another way.
3. *Attention* — passwords do not echo to the user interface, which is necessary to maintain the secrecy of the password but it is very difficult for users with a short attention span to keep track of what they have already typed without any visual cues. Thus one should ask users to identify particular items on the screen and use their ability to use this faultlessly to authenticate them.
4. *Dexterity* — passwords require the ability to type correctly, something that becomes increasingly difficult with age-related diseases such as arthritis and tremors. Hence one should ask them to use the mouse and click once only.
5. *Vision* — passwords do not rely on vision and any alternative we choose should ensure that those with failing vision can still easily use it.
6. *Special Requirements* — we should not require either extra hardware or software.
7. *Learning* — the system should be as easy to use as the password so as not to increase anxiety, not to apply an extra burden of learning something new, and it should let users down gently if errors do occur.
8. *Anxiety* — when users forget their passwords many systems now email their password to them so that there is no longer any shame attached to the loss of the key. The replacement of any alternative key should be as simple. One should be very wary of questioning older users about failures to authenticate since for some of the more computer illiterate since their sense of inadequacy in the digital world might lead them to consider this to be an inquisition and they could easily become distressed. (O'Neill 2000).

The Handwing system, mentioned in the identification discussion, attempts to address most of these issues. Handwing users authenticate based on recognition, not recall. Furthermore, Handwing uses a biometric — handwritten numerals — which act as a tailored cue for each user, as discussed in Section 3. Numerals are less specific than handwritten characters but also deliver a fair amount of individuality, as can be seen from the sample in Figure 2. Users being authenticated by Handwing progress through a 3-stage process:

1. The first screen presents the user with a selection of 10 PIN numbers, each written in a different handwriting, as shown on the left in Figure 3. The user is assisted in choosing the correct PIN by recognition of his or her own handwritten digits.
2. Once the user chooses one of the options the next page displays 10 postal codes, each in the handwriting of a different user, as shown on the right in Figure 3. The user chooses his or her own postal code.
3. The final screen displays 12 hand-drawn doodles as shown in Figure 4 — one of which belongs to the user. The user chooses his or her own doodle and is allowed to enter the site if all target images have been correctly identified.

The following section presents details about a long-term evaluation of a website with an authentication mechanism that implements these ideas.

0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9

Figure 2: Sample Numerals

94716	34387	91927	FK4 16Y	G11 5EB	G3 8PW.
05740	03527	48261	G75 8HL	ML8 5TY	G20 8QJ
16182	32842	65602	G12 8RZ	G38QX	MLS 454
	67276			G81 2HS	

Figure 3: Stage 1 and 2

Figure 4: The Doodle Stage

4 Long-Term Evaluation

A website was implemented for a church, and since the data held is private, but not sensitive, a medium to low strength authentication mechanism was required. Many of the church members are over 60 years of age and it was decided to test the recognition of handwriting for this website’s authentication mechanism. In order to use the authentication system, called HandWing, there is a one-time set-up process.

Figure 5: *Enrolment Form*

The user must provide his or her handwritten digits and postcode. He or she also provides a hand-drawn doodle. All users can be assumed to access the website from home, and most are using dial-up access. Members register by filling in a form, shown in Figure 5, which allows us to record their handwritten digits and doodle. Specially tailored identification and authentication mechanisms were developed for this website. The details are given in Sections 3.1 and 3.2. The website has now been running for 2 years with semi-regular usage by various users. The demographics of the current site users are: 55 site users altogether of which 24 are female and 31 male. The age groupings are as shown in Table 4.

	Under 19	20-29	40-49	50-59	Over 60
Female	6	3	4	7	12
Male	3	2	1	7	11

Table 1: Demographics

The site is not used heavily, but when we look at accesses over the two years, the semi-regular users² can be grouped as shown in Table 4.

	Under 19	20-29	40-49	50-59	Over 60
	2	2	3	7	14

Table 2: Semi-Regular Users

Initial experiences of the Handwing authentication system were provided in (Renaud 2005). The site has now been running for over two years and this paper reports on the evaluation of further work undertaken to refine the system and improve its usability. The identification and authentication mechanisms were evaluated separately and the results of the evaluation are presented in the following two sections.

4.1 Identification Evaluation

The new identification regimen was implemented and an evaluation carried out after six months. During this time users attempted to identify themselves 758 times. These were dealt with as illustrated in Figure 6. There was an obvious preference for email addresses as identifiers, with 597 visitors choosing to identify by means of an email address. Of these, 73 did not match to one of the member email addresses and had to be resolved. The software identified 36 of these by means of the approximation process — the rest were unresolved and the user was requested to attempt identification again. Non-email identifiers were not unique in 26 cases, and these were resolved in 17 cases by means of the approximator software. There were 45 cases where the proffered identification could not be resolved. These can be classified as follows:

- More than 3 characters missing or incorrect (25)
- Intruder email or rubbish entered (21)

²More than 10 accesses during the evaluation period

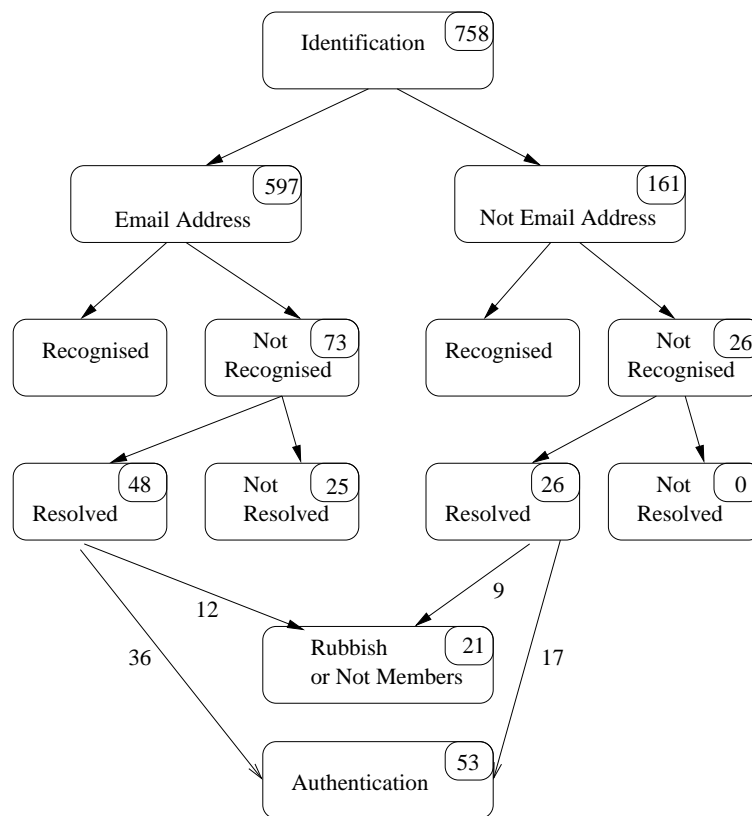


Figure 6: Identification

The only people who could not identify themselves, to the system’s satisfaction, were obvious intruders and people who entered addresses with more than 3 characters missing. It is entirely possible to adjust the approximator so that it is more lenient and permits addresses with even more characters wrongly typed or missing. One needs to exercise caution in this area, since one has to walk a fine line between ease of use and security and one does not want to open the system to attacks by intruders. However, the approximator did resolve addresses in 76% of cases, which justifies its use and eases the need for perfect typing skills

4.2 Authentication Evaluation

The web site has been running for 2 years during which there have been 1276 logins with only 25 (2%) episodes where users failed to log in at the first attempt. During these login episodes just over a half entered the website at the second or third attempt with only 12 (1%) attempts leading to abandonment. It is interesting to note that of the people who had difficulty logging in, 10 were over 60, 5 over 50 and only 1 in the 20 to 30 year age group. The difficulties experienced are summarised in Figure 7.

Most difficulties are related to identification of the PIN. There are some errors where users chose the wrong postcode or doodle but the evidence suggests that most users had difficulty identifying their PIN. One can often only surmise why the wrong item was chosen. All one can do is to examine the displayed items carefully and attempt to come up with a satisfactory explanation for the error. Errors are now discussed per category.

Postal Codes — This stage relies on the person’s own postal code, which makes errors during this stage puzzling. In one of the cases the incorrectly chosen postal code had some similarity to the person’s postal code and, if fleetingly considered, could have led to the error. The other two chosen postal codes were completely different from the user’s postal code.

Doodles — This stage relies on the user’s previous action-planning structures. All the doodle errors were examined since there was some concern that people could have been confused by similar-appearing doodles or doodles with the same semantic. The wrongly chosen doodle, *in all cases*, was completely different from the correct doodle. It could mean that they had forgotten their doodle, or it could mean they clicked too hastily or clicked in the wrong place by accident or clicked twice on the previous page, which was then accepted by the system as a click on the doodle page. The latter error has often been observed when people with limited computer use are not sure when to single-click and when to double-click.

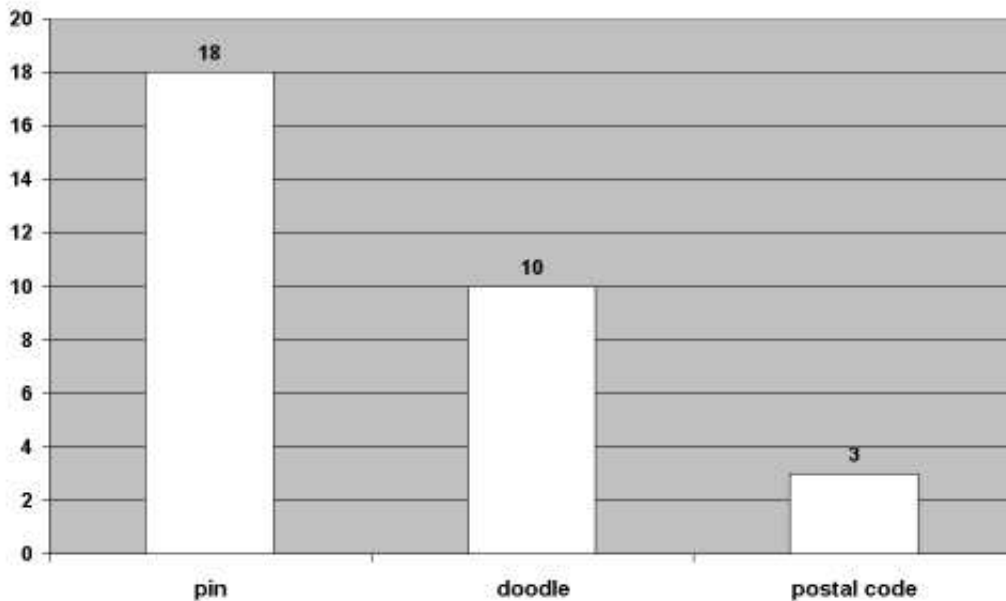


Figure 7: Authentication Errors

PINs — this, the most frequently occurring problem, is the most difficult to analyse, since the intention during this stage is that users rely mostly on recognition of their own handwriting. Similarity is in the eye of the beholder, and we can only speculate as to the reasons why the incorrect PINs were chosen. It could be that:

- the users were not using handwriting recognition to identify their PIN but rather trying to recall the PIN. It would be a simple matter to train these users but there are two problems with this. If a user is contacted and told that he needs training because he had failed to authenticate, this might dent his confidence and cause him to give up using the site altogether. The whole rationale behind this authentication mechanism is that users should be able to use it with minimal intervention, since that is really the acid test for a new mechanism. Therefore we are reluctant to intervene by training users.
- they could be mistaking the other PIN for theirs. The database has 151 different handwriting samples which are used randomly at login time. It is therefore entirely possible that the distractors are simply too similar to the target handwriting, especially if non-individualistic numbers, such as a 1 or 7, are used.
- they simply made a mistake. (To err is human!)

The similarity problems can be addressed by using similarity-predicting software. We are currently working on software which will choose distractors more intelligently so that users are not distracted by handwritings that are too similar to their own. We are also developing software to eliminate too-similar doodle distractors. It is interesting to note that, *without exception*, all users with failed attempts returned to the website and authenticated successfully at a later date. The other users, even with relatively infrequent use, are almost universally able to authenticate without difficulty.

In Section 3.2 a number of specific areas were identified that should be considered when developing an authentication mechanism for older users. It is now possible to evaluate the Handwing system in terms of these:

1. *Memory* — Handwing relies on recognition and not on faultless recall.
2. *Hearing* — Handwing does not use sounds.
3. *Attention* — users identify particular images and do not have to generate any keys themselves.
4. *Dexterity* — users point to images by clicking on the particular image.
5. *Vision* — the images are displayed prominently and only a minority of users had some difficulty identifying their own images.
6. *Special Requirements* — there are no special requirements.
7. *Learning* — the system appears to be easy to use for most users. A small subset of users have some difficulties but without directly observing their use of the system it is impossible to determine what the problems are.

8. *Anxiety* — users are permitted to re-enrol should they forget their key. They do not have to contact any administrator to regain access to the system and this should prevent them feeling anxious about making mistakes.

The three traditional dimensions of usability (from the ISO 9241 standard) are:

1. *Effectiveness*: Users were able, with only a few exceptions, to gain access to the website at the first attempt. Thus in terms of effectiveness the mechanism is extremely usable.
2. *Efficiency*: the time-consuming use of multiple screens to authenticate was not an issue for this group of users and did not affect the usability of the mechanism.
3. *Satisfaction*: user opinions have been gathered twice since the website was deployed — once after 9 months and once after 18 months.

The following section discusses a questionnaire used to gauge the usability dimensions for this system at the second attempt. Only authentication was investigated since the identification mechanism is completely invisible to the users.

4.2.1 Questionnaire

At 18 months a questionnaire was displayed when the users logged in and they were asked to fill it in to give their opinions. One third of users responded. Users were asked to rate the logging in process in terms of security, ease of use, satisfaction, speed, fun, stress and efficiency on a scale of 1 to 5 with 1 indicating dissatisfaction and 5 complete satisfaction. Table 3 shows the averaged responses from 17 users. Responses were obtained from 10 females and 7 males. Nine of the respondents were over 60, seven were from the 50 to 60 age group and one from the 20 to 30 age group. As can be seen from the table, the lowest mean score for any of the variables was 3.8, which is above the neutral scoring midpoint of 3.

	How secure do you think the site is	How easy using handwriting	How satisfied are you with the logging in process?	Is logging in fast enough?	How much fun is it?	How relaxing is it?	How efficient is it?
N	17	17	17	17	17	17	17
Mean	4.4118	4.0000	4.4118	4.2353	3.8824	4.4118	4.6471

Table 3: Results of Questionnaire. 1=dissatisfaction, 5=complete satisfaction

No significant differences were found when the 50-59 age group and the 60 plus age group were compared. No data was collected to determine the efficiency of the mechanism since time constraints did not appear to be important to this group of users. However, when the respondents were asked whether they would prefer the system to change to use passwords rather than the Handwing process, not one respondent indicated that such a change would be desirable. These initial findings from the usability evaluation of the Handwing mechanism indicate that it satisfactorily meets the requirements stated in this paper, both in terms of the ISO standard and the needs of the target user group.

5 Conclusion

This paper discusses issues related to the identification and authentication of older web users. A website was developed to serve a small community of users, with a wide range of ages. This meant that the mechanism controlling access had to be chosen with great care, to encourage repeat visits. Although such users can make use of passwords quite successfully if they employ some strategy, such as writing it down, passwords simply have too many disadvantages for a group of users with such wide-ranging abilities and disabilities, protecting a low-risk site.

A specially tailored web authentication mechanism, called HandWing, was deployed to meet the needs of the users and evaluated by means of logging accesses and obtaining user self-reports. The HandWing mechanism is weaker, more memorable and definitely more usable than passwords. Handwing does not claim to be perfect — as evidenced by the errors reported in the evaluation. It does claim to be a viable alternative, which appears to reduce problems at authentication, and it is also obviously acceptable to its users.

It is high time that target user groups are considered in identification and authentication and that some attention is paid to ensuring the usability of these essential parts of the user interface, as is routinely done for other parts of the website.

References

AKATSU, H. & MIKI, H. 2004, Usability Research for the Elderly People , *Oki Technical Review* **71**(3), 54–57.

- BECKER, S. A. 2004, A study of web usability for older adults seeking online health resources , *ACM Transactions on Computer-Human Interaction* **11**(4), 387–406.
- BOTWINICK, J. 1967, *Cognitive processes in maturity and old age*, Springer, New York.
- BRENNAN, Z. 1997, Oldmobiles roll up for grey drivers , *The Sunday Times*. 28 December, page 13.
- BROSTOFF, S. & SASSE, A. 2000, Are passfaces more usable than passwords? a field trial investigation, in S. McDONALD, ed., *People and Computers XIV - Usability or Else! Proceedings of HCI 2000* , Springer, pp. 405–424.
- CATTAN, M., WHITE, M., BOND, J. & LEARMOUTH, A. 2005, Preventing social isolation and loneliness among older people: a systematic review of health promotion interventions , *Ageing and Society* **25**(3), 357–76.
- CHADWICK-DIAS, A., McNULTY, M. & TULLIS, T. 2003, Web usability and age: how design changes can improve performance, in *Proceedings of the 2003 conference on Universal usability*. November 10-11 , Vancouver, British Columbia, Canada, pp. 30–37.
- CHEN, H. L. 1994, Hearing in the elderly. relation of hearing loss, loneliness, and self-esteem , *Gerontological Nursing* **20**(6), 22–8.
- CHISNELL, D., LEE, A. & REDISH, J. 2004, Design Web Sites for Older Users: Comparing AARP's Studies to Earlier Findings . <http://www.aarp.org/olderwiserwired/oww-features/Articles/a2004-03-03-c%omparison-studies.html> . Retrieved 13 April 2005.
- CHISNELL, D. & REDISH, J. 2005, Who is the Older Adult in your Audience? , *intercom* . http://www.stc.org/intercom/PDFs/2005/200501_10.pdf . Retrieved 13 April 2005.
- CLARK, D. J. 2002, Older adults living through and with their computers , *CIN: Computers, Informatics and Nursing* **20**(3), 117–124.
- COHEN, G. & BURKE, D. M. 1993, Memory for proper names: a review , *Memory* **1**, 249–263.
- COX, B. 2002, Hijacking and fraud plague ebay users , *ECommerce*. <http://www.internetnews.com/ec-news/article.php/1480591> . Accessed 21 Nov 2005.
- CRAIK, F. & BIALYSTOK, E. 2006, Cognition through the lifespan: mechanisms of change , *TRENDS in Cognitive Sciences* **10**(3), 131–138.
- CZAJA, S. J. 1996, Aging and acquisition of computer skills, in W. A. ROGERS, A. D. FISK & N. WALKER, eds, *Aging and Skilled Performance: Advances in Theory and Applications* , Lawrence Erlbaum Associates, Inc, pp. 201–221.
- DE ANGELI, A., COUTTS, M., COVENTRY, L. & JOHNSON, G. I. 2002, VIP: A Visual Approach to User Authentication, in *Proceedings of the Working Conference on Advanced Visual Interfaces AVI. 2002* , ACM Press, pp. 316–323.
- DE ANGELI, A., COVENTRY, L., JOHNSON, G. & RENAUD, K. 2005, Is a picture really worth a thousand words? Reflecting on the usability of graphical authentication systems , *International Journal of Human-Computer Studies: special issue: HCI research on Privacy and Security* **63**(1-2), 128–152.
- DELOITTE 2005, Global security survey . [http://www.deloitte.com/dtt/cda/doc/content/us_fsi_150606globalsecurity%survey\(1\).pdf#search=%22global%20security%20survey%20deloitte%22](http://www.deloitte.com/dtt/cda/doc/content/us_fsi_150606globalsecurity%survey(1).pdf#search=%22global%20security%20survey%20deloitte%22) . Accessed: September 2006.
- DENING, T. & BARAPATRE, C. 2004, Mental health and the ageing population , *The Journal of the British Menopause Society* **10**(2), 49–53.
- DHAMIJA, R. & PERRIG, A. 2000, Déjà vu: A user study using images for authentication, in *Proceedings of USENIX Security Symposium* , Denver, Colorado, pp. 45–58.
- DORAN, G. D. 1999, Touchy subject-biometric technology: Is it time for your computer to get to know you? , http://www.findarticles.com/p/articles/mi_m0DTI/is_4_27/ai_60036365 . Accessed: September 2006. Entrepreneur magazine.
- DTI 2005, Information security factsheet . Department of Trade and Industry. <http://www.dti.gov.uk/files/file9937.pdf?pubpdfload=05%2F612> . Accessed: September 2006.
- ENGARDIO, P. & MATLACK, C. 2005, Global aging . *Business Week*, JANUARY 31, http://www.businessweek.com/magazine/content/05_05/b3918011.htm . Accessed: September 2006.
- FOX, S. 2001, Wired seniors. a fervent few, inspired by family ties, Technical report, Pew Internet and American Life Project. http://www.pewinternet.org/pdfs/PIP_Wired_Seniors_Report.pdf . Accessed May 2006.
- GILL, J. 2004, Design of Smart Card Systems to Meet the Needs of Disabled and Elderly Persons . Tiresias.org Scientific and Technological Reports. <http://www.tiresias.org/reports/ecart.htm> . Accessed: September 2006.
- GOLDBERG, E. 2005, *The Wisdom Paradox*, Gotham Books.
- GOODMAN, J., BREWSTER, S. & GRAY, P. 2004, Connecting elders by facilitating mobility, in *Position paper at workshop on Home Technologies to Keep Elders Connected at CHI 2004* , Vienna, Austria.
- HAWTHORN, D. 2000, Possible implications of aging for interface designers , *Interacting with Computers* **12**, 507–528.
- HAWTHORN, D. 2003, How universal is good design for older users?, in *CUU '03: Proceedings of the 2003 conference on Universal usability* , ACM Press, pp. 38–45.
- HECKMAN, J. G., LANG, C. J. & NEUNDORFER, B. 2001, Recognition of familiar handwriting in stroke and dementia , *Neurology* **57**(11), 2128–31.
- JACKSON, G. R. & OWSLEY, C. 2003, Visual dysfunction, neurodegenerative diseases and aging , *Neurology and Clinical Neurophysiology* **21**(3), 709–28.

- KELLEY, C. L. & CHARNES, N. 1995, Issues in training older adults to use computers , *Behaviour and Information Technology* **14**, 107–120.
- KIEL, J. M. 2005, The digital divide: Internet and e-mail use by the elderly , *Medical Informatics and the Internet in Medicine* **30**(1), 19–23.
- KNOBLICH, G. & PRINZ, W. 2001, Recognition of self-generated actions from kinematic displays of drawing , *Journal of Experimental Psychology: Human Perception and Performance* **27**, 456–465.
- LAGUNA, K. & BABCOCK, R. 1997, Computer anxiety in young and older adults: Implications for human computer interactions in older populations , *Computers in Human Behavior* **13**(3), 317–326.
- LEVENSHEIN, V. I. 1965, Binary codes capable of correcting deletions, insertions and reversals , *Doklady Akademii Nauk SSSR* **163**(4), 845–848. also Soviet Physics Doklady 10(8) p707-710, Feb 1966.
- LINDEMAN, E. 1947, Methods of democratic adult education, in S. BROOKFIELD, ed., *Learning Democracy: Eduard Lindeman on Adult Education and Social Change* , Croom Helm, London., pp. 53–59.
- LOGAN, J. M., SANDERS, A. L., SNYDER, A. Z., MORRIS, J. C. & BUCKNER, R. L. 2005, Under-recruitment and nonselective recruitment: dissociable neural mechanisms associated with aging , *Neuron* **33**(5), 827–840.
- LONGCAMP, M., ANTON, J. L., ROTH, M. & VELAY, J. L. 2003, Visual presentation of single letters activates a premotor area involved in writing , *Neuroimage* **19**(4), 1492–500.
- MADDOX, G. & DOUGLAS, E. 1974, Aging and individual differences , *Journal of Gerontology*, **29**, 555–563.
- MATHER, M. & CARSTENSEN, L. 2005, Aging and motivated cognition: the positivity effect in attention and memory , *TRENDS in Cognitive Sciences* **9**(10), 496–502.
- MAZAUX, J. M., DARTIGUES, J. F., LETENNEUR, L., DARRIET, D., WIART, L., GAGNON, M., COMMENGES, D. & BOLLER, F. 1995, Visuo-spatial attention and psychomotor performance in elderly community residents: effects of age, gender, and education , *Journal Clin Exp Neuropsychol* **17**(1), 71–81.
- MCAVOY, L. 1979, The leisure preferences, problems, and needs of the elderly , *Journal of Leisure Research* **11**(1), 40–47.
- MCCRAE, N., MURRAY, J., BANERJEE, S., HUXLEY, P., BHUGRA, D., TYLEE, A. & MACDONALD, A. 2005, They're all depressed, aren't they? A qualitative study of social care workers and depression in older adults , *Aging Mental Health* **9**(6), 508–16.
- MCMELLON, C. A. & SCHIFFMAN, L. G. 2002, Cybersenior empowerment: How some older individuals are taking control of their lives , *Journal of Applied Gerontology* **21**(2), 157–175.
- MERRIAM, S. B. & CUNNINGHAM, P. M., eds 1990, *Handbook of adult and continuing education*, Jossey, Bass. San Francisco.
- MORRIS, J. M. 1994, Computer training needs of older adults , *Educational Gerontology* **20**, 541–555.
- NIA & NLM 2002, Making your web site senior friendly, Technical report, National Institute on Aging and National Library of Medicine. <http://www.nlm.nih.gov/pubs/checklist.pdf>. Accessed May 2006.
- O'NEILL, L. 2000, The implications of an aging population on interface design, Master's thesis, Department of Informatics, Sussex University.
- PENNEBAKER, K. & STONE, L. 2003, Words of wisdom: Language use over the life span , *Journal of Personality and Social Psychology* **85**(2), 291–301.
- PFLIEGER, C. P. & PFLIEGER, S. L. 2003, *Security in computing*, 3 edn, Prentice Hall, Upple Saddle River NJ.
- POKOMY, J., SMITH, V. C. & LUTZE, M. 1987, Aging of the human lens , *Applied Optics* **26**, 1437–1440.
- RANZI, R., KEEVES, J., LUSZCZ, M. & FEATHER, N. T. 1998, The role of self-perceived usefulness and competence in the self-esteem of elderly adults: confirmatory factor analyses of the bachman revision of rosenberg's self-esteem scale , *Psychological Sciences and Social Sciences* **53**(2), 96–104.
- RASH, W. 2002, Password chaos threatens e-commerce , ZDNet. <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2847895,00,%html>. Accessed: September 2006.
- RENAUD, K. 2005, A visuo-biometric authentication mechanism for older users, in Proc British HCI 2005. Sept 5-9, Edinburgh , pp. 167–182.
- RENSINK, R. A. 2002, Change detection , *Annual Review of Psychology* **53**, 245–277.
- ROBERTS, P. 2001, Electronic media and the ties that bind , *Generations* **25**(2), 96–98.
- SALTHOUSE, T. A. 1985, Speed of behavior and its implications for cognition, in J. E. BIRREN & K. W. SCHAIKE, eds, *Handbook of the psychology of aging* (2nd edition) , New York: Van Nostrand Reinhold, pp. 400–426.
- SEKI, K., YAJIMA, M. & SUGISHITA, M. 1995, The efficacy of kinesthetic reading treatment for pure alexia , *Neuropsychologica* **33**(5), 595–609.
- SHAPIRO, P. 1995, Computers use and the elderly , Web Document. Written for the Washington Apple Pi Journal. <http://www.his.com/~pshapiro/computers.and.elderly.html>. Accessed: September 2006.
- SRIHARI, S. N., CHA, S.-H., ARORA, H. & LEE, S. 2001, Individuality of handwriting, in Proceedings of the Sixth International Conference on Document Analysis and Recognition (ICDAR 01) , IEEE Computer Society, Seattle, WA, pp. 106–109.
- STANKOV, L. 1988, Aging, attention and intelligence , *Psychol Aging* **3**(1), 59–74.

- STEWART, T. 1997, Why do older workers have problems with technology? , *Journal Human Ergol* **26**(2), 185–92.
- TIMMERMAN, S. 1998, The role of information technology in older adult learning , *New Directions for Adult and Continuing Education* **77**, 61–71.
- TREISMAN, A. & DAVIES, A. 1976, Dividing attention to ear and eye, in S. KORNBLULM, ed., *Attention and Performance* , Academic Press, New York, pp. 101–117.
- TROSTEL, P. A. & TAYLOR, G. A. 2001, Theory of time preference , *Economic Inquiry* **39**(3), 379–395.
- VAN IWAARDEN, J. & VAN DER WIELE, T. 2003, Applying SERVQUAL to web sites: an exploratory study , *International Journal of Quality & Reliability Management* **20**(8), 919–935.
- W3 1999, Web content accessibility guidelines . World Wide Web Consortium. <http://www.w3.org/TR/WAI-WEBCONTENT/>. Accessed: September 2006.
- WALKER, T. 2001, Fighting security breaches and cyberattacks with two-factor authentication technology , *Information Systems Control Journal* **2**. <http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=17187&TEMPLATE=/ContentManagement/ContentDisplay.cfm>.
- WEINSHALL, D. 2004, Secure authentication schemes suitable for an associative memory, Technical Report TR 2004-30, Hebrew University, Leibniz Center for Research in Computer Science.
- WITTY, R. J. & BRITAIN, K. 2004, Automated password reset can cut it service desk costs . Gartner Report.
- ZIMMER, A. 1982, Do we see what makes our script characteristic —or do we only feel it? Modes of sensory control in handwriting , *Psychological Research* **44**(2).