

Web Authentication using Mikon Images

Karen Renaud

Department of Computing Science

University of Glasgow

Glasgow, United Kingdom

karen@dcs.gla.ac.uk

Abstract—Authentication is mostly achieved by means of the ubiquitous password. This is suboptimal in some settings, such as for user groups with cognitive or language difficulties. Many web-based systems have user groups with widely ranging capabilities, and more innovative authentication mechanisms should be investigated to enhance usability and accessibility while still delivering the required level of security to authorise legitimate users.

This paper presents details of an authentication system which relies on the user identifying previously drawn *Mikons*¹. Mikons are self-drawn icon-like images, meant to depict a message the artist wants to convey at that point in time. These are drawn, at enrolment, using an embedded ShockWave component within a browser. At authentication the user identifies his or her own Mikons from challenge sets, each containing one of the user's Mikon and a number of distractor Mikons.

The efficacy of Mikons in this setting was investigated by using them in a recognition-based authentication system to authorise users of an online homework system over an eight month period. The Mikon-based system performed very well in terms of memorability and scalability, as anticipated, thus achieving the level of accessibility hoped for. A measure of predictability was observed, with a few of the participants being able to link sets of Mikons to their creators; but this did not pose a security risk to the system.

This study shows that Mikon authentication has the potential to be a viable alternative to passwords for systems where the security requirement is secondary to other, more important, considerations. Such systems are usually low-risk and are often used by users with developmental, language or cognitive difficulties, or by users who are not yet literate. The imposition of a password on such users can be overly stringent and excessively demanding in terms of scarce cognitive resources. In this context, therefore, Mikons are a viable alternative to meet the needs of the target user group.

Keywords — Authentication, Accessibility, Mikons.

I. INTRODUCTION

When access to an electronic resource is restricted, legitimate users need to prove that they are entitled to access it. They do this by proffering an identity, and the identity is verified by means of an authentication step. This ensures individual accountability, auditability of actions and non-repudiation of the same.

The most common way for computer users to be authenticated is by means of a shared secret called a password, a concept that goes back thousands of years. This is commonly referred to as *knowledge-based authentication* — a shared secret between authenticator and authenticated. Unfortunately,

as the use of the Web increases, users have to remember vast numbers of passwords [1], [2]. Human memory limitations make the forgetting of such passwords inevitable. People know that they will forget passwords, especially those used infrequently, and this makes them either choose weak passwords, use the same password for all systems or write them down [3].

Even if users are extremely motivated to behave securely, and don't fall into the above-mentioned traps, passwords remain inaccessible to many users. The password is essentially a word which has to be entered via the keyboard. Consequently, anyone who has a problem with words, language, dexterity or remembering random sequences of characters is going to find passwords a challenge. They then become a major hurdle, which may well prevent the legitimate user from accessing the system. Quite common disabilities such as such as dyslexia² (15% of the population) and dyspraxia³ (10% of the population). Dyslexia is a learning difficulty which affects language related skills. Affected people will have difficulty with reading, spelling and working memory. Dyspraxia is a disability that affects the way the brain processes information. It specifically impacts on language and thought processes. People with these disabilities will experience difficulties with passwords.

Furthermore, some groups of users simply haven't yet progressed to the level of cognitive processing which the password requires. This could be due to developmental lags or deficits and it is ill-advised to impose a password requirement on such groups when the real object of accessing the system is usually to provide an educational experience which has nothing to do with remembering the password itself.

In addressing the authentication accessibility problem, the proposal here is that we make use of an *alternative* approach which relies on recognition rather than on recall, a less demanding requirement [4]. A user can be asked to recognise his or her secret from a group of possibilities, rather than to recall and enter it without any assistance or cues.

Graphical authentication mechanisms rely on recognition of images rather than recall of alphanumeric passwords, since people purportedly recognise a picture better than they recall an alphanumeric string with the same amount of detail [5], [6], [7]. This relies on the much vaunted *picture superiority* effect [8], which argues that people remember pictures better because

¹www.mikons.com

²www.interdys.org

³www.dyspraxiafoundation.org.uk

they employ a dual-coding strategy when seeing pictures: storing at least the visual aspect as well as a verbal label in their memory, as opposed to a simple word in the case of passwords.

The use of images for this purpose is particularly useful in particular settings, such as those where the intended users of the system are illiterate [9], have poor reading skills [10], use a different alphabet [11] or have short term memory problems [12].

Some image genres are not well-suited for this purpose. The characteristics of the pictures used by the authentication mechanism impacts on both the memorability and the security of the mechanism [13]. Researchers sometimes solve the one aspect at the expense of the other. For example, research using the user's own home photographs [14], [15] proved the superior memorability of photos. Unfortunately this fails to consider the risk associated with the ease of someone guessing the link between the photo and the user — all too easy if personal photos are used. Lim *et al.* propose a taxonomy of home photos [16], which classifies personal photos into one of *gathering*, *family activities*, and *places visited*. The first two categories are likely to include pictures of people related in some way to the photographer, and this will increase predictability.

What is required, therefore, is an image which is memorable but not easily linked to the user. However, memorability is not the only consideration, but also the accessibility of the mechanism to a user base with widely ranging cognitive and language skills.

Section II discusses the efficacy of different image types, and explains why the Mikon image was chosen for this study. Section III details the design and implementation of the authentication software system. Section IV presents the results of the evaluation and Section V discusses the results and Section VI outlines future work to be undertaken. Section VII concludes.

II. IMAGE EFFICACY

This section will present a discussion of the efficacy of images for use in graphical authentication. Since memorability is the main problem being focused on in this paper, this is discussed first.

A. Memorability

Some pictures perform better than others in graphical authentication. In the Déjà vu system [17], the photographic images proved to be more memorable than the abstract art images. In an experiment where photographic images, home photos and hand-drawn pictures were compared, hand-drawn pictures were remembered better than the others [13]. The literature provides some compelling reasons for this. In the first place, there is much evidence that we remember things we do — our actions — very well. As Dixon and Glover [18] state, “action is memory”. Zimmer and Cohen [19] claim that the memory of actions is a by-product of their execution, which means that the action of encoding that memory is probably involuntary and implicit rather than explicit and effortful.

When someone is drawing a picture he or she is engaging in actions, and it is clear from the literature that humans have a superior memory for self-performed tasks [20], [21], [22].

Nyberg and Nilsson [23] proved that, in general, self-performed tasks are remembered better than verbal materials. Knopf *et al.* [24] showed that verbal encoding, which one can expect when a picture is viewed (based on the picture superiority effect [8]), is not as effective as the memory encoding that occurs based on action-planning processes.

It is not even necessary for a person to repeat the same actions for the initial memory to “fire”. For example, Knoblich and Prinz [25] observed that people could recognise their own drawings even when they did not get visual feedback when they drew the pictures initially.

The drawing process involves a number of senses including vision and touch, and also the feedback from motor activities as the drawing progresses, with various sensory inputs giving continuous feedback to guide the drawing process. Sensory processes turn out to be essential in laying down memories during actions. Leynes *et al.* [26] showed that sensory characteristics provided unique information for action memories, and that this sensory information was often activated when the action was remembered. This finding appears to be confirmed by the findings of other researchers:

- Longcamp *et al.*, [27] who found that when people read letters of the alphabet they had previously written, the same regions of their brains that were activated by the writing process, were re-activated.
- Pianists can recognise recordings of their own performances, even when the sound is removed during the initial recording of the performance [28].
- Flach *et al.* reports that people can identify their own clapping [29].
- Loula *et al.* [30] proved that people were best at identifying their own movement, even in poor lighting conditions, when they saw videos of their own, their friends' and strangers' movements.

These examples all refer to memory for motor skills. In the context reported here the only motor skill used would be the mouse movement, and this is probably too generic to rely on. However, Foley and Ratner [31] do not consider the use of sensory inputs which result from motor skills to enhance the memorability, but argue that the *goal-directed* nature of an activity is what ensures that strong memory traces are laid down. Zimmer [20] enumerates a number of aspects of such goal-directed activity that ensure the superior strength of this memory trace:

- they are planned,
- their execution produces an outcome which can be perceived and assessed, and
- they are composed of a sequence of sub-part actions.

When the person remembers activities previously carried out, memories of the action planning process will come to mind. A related finding is that doodling while listening to someone speaking actually helps the listener to retain what was said better than if they did not doodle [32]. This finding seems to confirm that the memorial advantages of engaging in actions

are not confined to memories of the actions themselves.

There is a strong case for concluding that it is better actively to engage than merely to look, if a strong memory trace is desired. There is also evidence that, having carried out the action, one can expect enhanced recognition performance of any artifact related to the original action [33].

B. From Drawings to Mikons

Research cited in the previous section has shown that drawings are memorable, and long term trials of the use of drawings in authentication have delivered positive results [12]. Unfortunately, there is a drawback with the use of a drawing in digital authentication and that is that the system does not scale well — drawings have to be scanned in manually and converted to digital images and then uploaded into the system. This is time-consuming and not viable for large scale usage.

The research reported in this paper was carried out in order to test the viability of on-screen drawings in authentication. If it is possible to have users draw their own images digitally and the system is able then automatically to enrol them, the human is removed from the process, and the system becomes scalable. This study used the Mikon Engine, developed by the Mikons.com company, to facilitate drawing of an on-screen image. The engine facilitates drawing of an icon-like picture within a browser, which makes this mechanism particularly suitable as a Web authentication tool. Mikon is short for *my icon* and is a way for people to express themselves. Their website describes a Mikon as being *a symbol about you*, which can represent just about anything you're thinking about at the time you're drawing it. The central idea behind Mikons is to encourage people to draw and share Mikons, using them in both the virtual and real worlds. The use of Mikons in authentication is completely different, requiring a measure of dissemblance from the person drawing the Mikon so that artist attribution becomes difficult.

On the other hand, the memorability advantage of hand-drawn pictures should be equally strong for Mikons since they are the result of a goal-directed series of actions undertaken by the person drawing the Mikon. Fortunately, since people can draw Mikons in their browser, it should be possible to automate much of the enrolment process, thereby avoiding the main disadvantage of hand-drawn picture-based systems.

Based on this discussion we can reasonably expect self-drawn Mikon images to have superior memorability and they do not suffer from the scalability problems that drawings do. The final question to be considered is the security of the mechanism. What can we expect in terms of security, specifically predictability? In other words, how easy will it be for other users to link the self-drawn image to the artist? The next section addresses these issues.

C. Artist Attribution

The obvious problem is that someone who knows a user well might be able to link the user to his or her drawn Mikons. The identification of the Mikons is made somewhat more difficult by the fact that they are displayed amongst 60 other Mikons. Identification of Mikons requires that the person

attempting to make the identification firstly understands what the drawer was attempting to convey using the Mikon, and secondly, reliably links the artist to the Mikon.

In contemplating shared understanding, it is worth considering what Sturken and Cartwright [34] have written about icon image types. They explain that icons, in this case Mikons, are particular image types which refer to something outside of the individual components thereof. The icon has a symbolic meaning to the creator of the icon, which may or may not be shared by other viewers. It is therefore reasonable to assume that a self-drawn icon brings with it hidden meanings which encompass the assumptions and attitudes of the drawer, at the time of drawing.

To understand the attribution issue — linking Mikons to artist — it is necessary first to consider that any drawn image has both a denotative and a connotative meaning [34]. The denotative meaning is literal and refers to its descriptive aspect. The connotative meaning, however, relies on a cultural and historical interpretation of the image. For example, a picture of a snake denotes an actual snake, perhaps a specific species such as a Cobra. The connotative meaning might well be “danger”. Sturken and Cartwright point out that a particular image can have multiple meanings to different people, depending on their cultural, social and political background and experience. Furthermore, the meaning can change over time, and is strongly dependent on context. Mathur [35] enumerates the following barriers to a shared understanding of a visual image:

- 1) *Personality differences*: humans are unique and differ in terms of their experience, communication abilities and intelligence, to mention a few aspects. Mathur points out that we learn to interpret what we see based on our experience and on what we have been taught. Furthermore, whereas some people are intensely visually oriented, others are verbalisers or spatialisers — people assimilate information primarily from their favoured mode of interaction.
- 2) *Perception filter*: perception is influenced by our needs and views. Mathur explains that people interpret only those aspects of an image which interest them.
- 3) *Context*: it is impossible to recreate the same context in the viewer's mind as was present in the image creator's mind at the time the picture is being drawn.
- 4) *Understanding*: Mathur explains that a viewer could easily interpret a visual in purely denotative terms, and completely miss the intended meaning thereof.
- 5) *Colour use*: colour use is extremely culture dependent. In Western society red denotes danger but is perceived as lucky in China. Mathur points out that colour preference is influenced by factors such as brightness, saturation, value, flavour of the day, gender and age, among others. The viewer's background will therefore influence the interpretation of the visual.

It is therefore not a given that one person will necessarily have the same understanding of a Mikon as the person who drew it or to gain an insight into their thought processes while it was being drawn. In this context, however, having

a shared understanding does not necessarily lead to reliable identification of the creator of the Mikon.

It is impossible to gauge, using only theory, the possibility of another person being able easily to identify the person who produced the Mikon. This can only be ascertained experimentally. An experiment to determine this is reported next.

III. MIKON AUTHENTICATION

An online homework system was developed for a class of 11 and 12 year old pupils and Mikon authentication was used to authenticate them.

There are a number of reasons why Mikon authentication was considered to be a preferable mechanism for this system:

- The pupils in this school are allocated a password at primary school as soon as they are able to read and write, and this is not changed throughout the pupils' school career unless the pupil requests a reset. This means that many passwords are very simple and easily guessed, and, over time, leaked to other pupils.
- Some of the pupils had language difficulties or developmental lags and deficits and had consequent difficulty with remembering and entering their passwords. The difficulty in entering the password occurred due to the obfuscation of the entered word during entry. Pupils could not see what letters they had already typed in, and they lost track of where they were. When the system rejected a password they often had no idea why this had occurred so could not correct their mistakes, a problem Schmidt *et al.* [10] experienced in their research as well.
- The online homework system was to be used to provide the pupils with formative feedback. Hence the important thing was for them to do the work and to gain some feedback about their understanding of the concepts. The use of a traditional password in this context, with its associated cognitive load, was considered less than optimal. Anything that would cause difficulties and prevent pupils from accessing the system would be detrimental and the teacher was willing to trial an alternative to passwords which would provide necessary and sufficient security, but no more.

The Mikon authentication system has three phases which need to be designed: enrolment, authentication and replacement. The process is illustrated in Figure 1, and these phases of Mikon authentication will be discussed in the following Sections.

A. Enrolment

1) *Preparation:* Pupils were added to the system by the teacher, who entered their names and email addresses. The pupils were then given an introductory talk, and the need for the secrecy of their authentication images was explained to them. They were then directed to the online homework system website to register.

2) *Registration:* Registration required them to draw 4 Mikons in succession. They used the Mikon engine, with the interface as shown in Figure 2, to draw one picture at a time. An example of a drawn Mikon is shown in Figure 3. Once

they had drawn their Mikons, they were told that they would receive an email message when their account had been created. An example of a set of Mikons drawn by the pupils is shown in Figure 4.

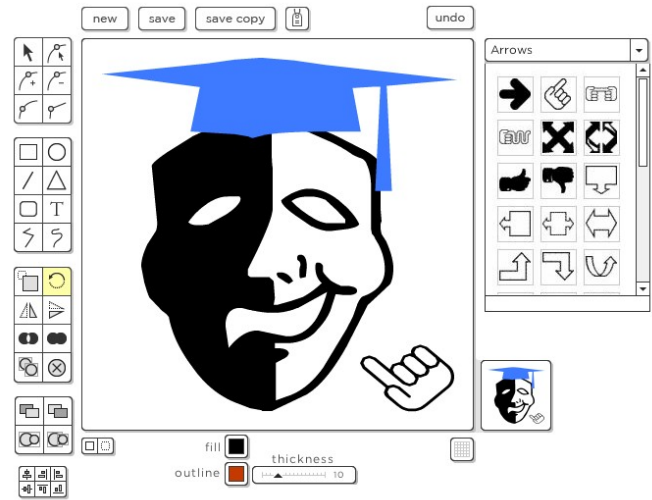


Fig. 3. Final Picture

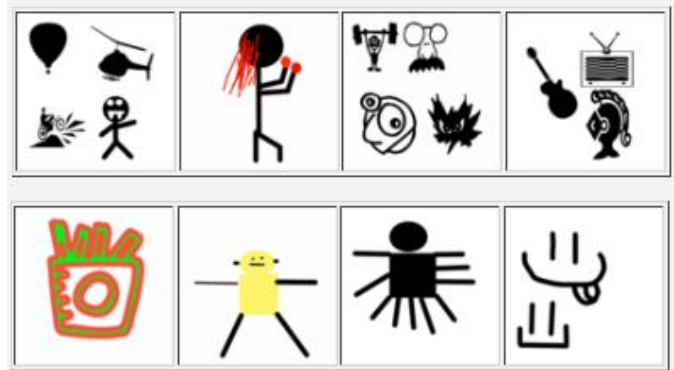


Fig. 4. Example Mikon Sets

3) *Approval:* The next step in the process was for the teacher to approve the pupil's Mikons. It is a requirement of any system that children make use of that unsuitable images are not permitted. The teacher can either approve the images or require the pupil to draw a new set of images if they are deemed to be unsuitable.

4) *Distractor Choice:* The next step is to choose the distractor images. We have an archive of over 2000 Mikons and distractor images suitable for a particular pupil's Mikon images need to be chosen. We have two options here: to vary the distractors at each authentication attempt or to choose the distractors at enrolment and use those for each attempt. Since Mikon authentication is being facilitated in a browser, we cannot vary the distractors since the refresh button would allow an intruder to identify the target picture as the only one that does not change with every page refresh.

It is also necessary to ensure that the distractors are not too similar to the target Mikon in each challenge set because that might cause confusion. A specially developed algorithm

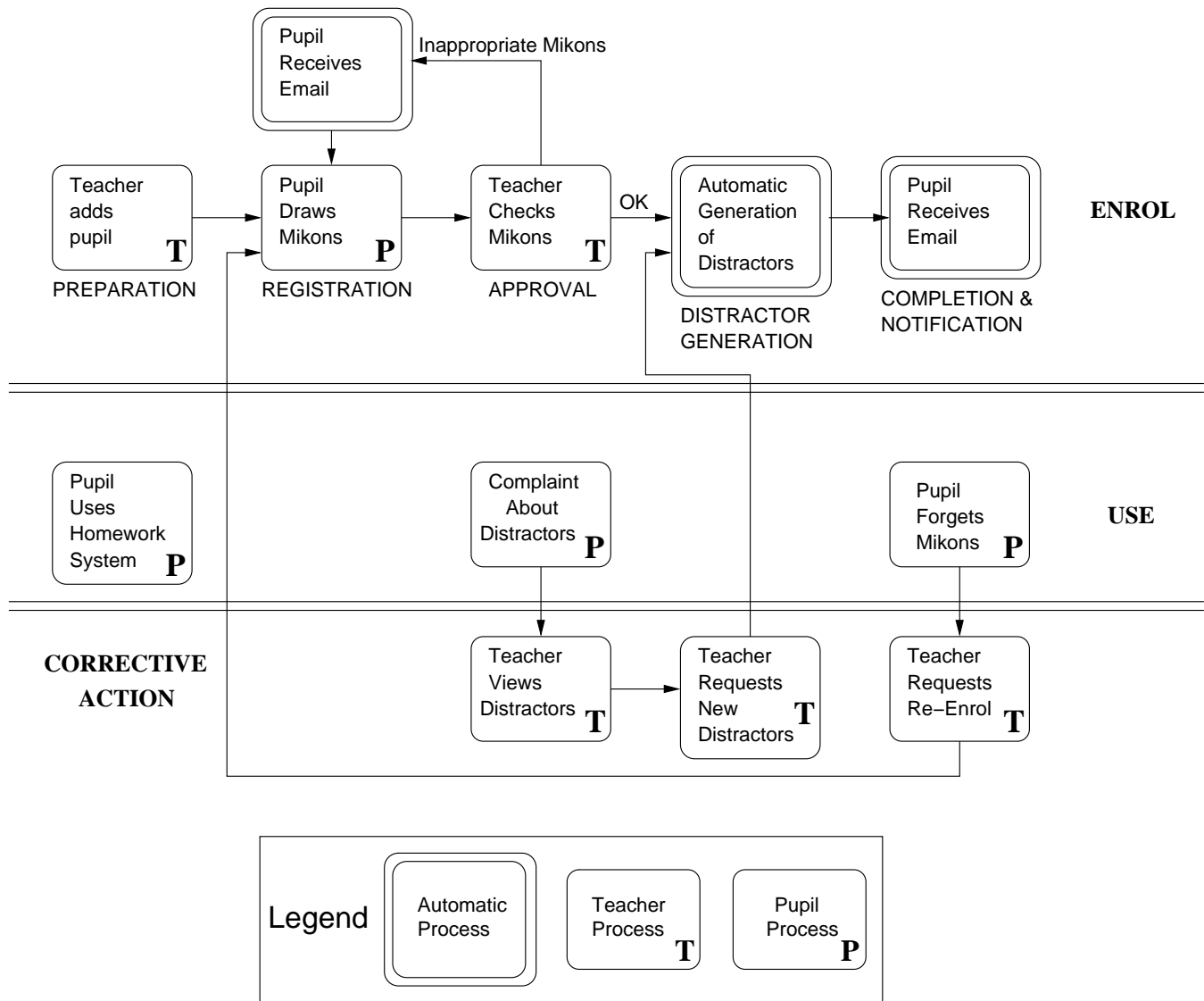


Fig. 1. Mikon Authentication Processes

chooses images based on the *visual appearance* of the target Mikons [36]. This process runs daily and generates the distractor images for each new account for which the Mikons have been approved. Similarity ratings can also be based on semantics or phonetics. So, for example, whereas a daffodil and a rose are visually different, they are from the same semantic category, which could cause confusion. Confusion could also result from pictures which start with the same digraph — for example, *dog* and *doll*. However, automating similarity ratings in terms of semantics or phonetics is difficult and expensive in terms of time and human involvement. The visual similarity algorithm, while not delivering perfect results, performs very well. Since it completely automates the process, it was the obvious choice for helping the system to choose dissimilar distractors automatically.

5) *Completion & Notification:* Finally, the pupil receives an email which informs him or her that the account has been created. The pupil is then free to complete homework assignments set by the teacher.

6) *Time & Resources:* The teacher is involved in this process, since he/she has to approve the Mikons. There is simply no way around this if one allows users to provide or draw images. A small percentage of users will always test the boundaries and a human agent needs to be involved to control this. The teacher was also the contact point in terms of allowing students to re-register in cases where they had forgotten their Mikons or to request new sets of distractors.

If the system is to be used by adults, the requirement for human approval of images can be relaxed, substituting it with a reporting system which deploys the users of the system as monitors. This serves to flag unsuitable images which can then be removed. In the system reported here this approach was unsuitable due to the age of the users.

An auxiliary web-based system was developed to allow the teacher to exercise full control over the system, with options to allow the adding and removing of pupils, entering homework and the carrying out of various other administrative actions. This system used a traditional strong password to authenticate teachers.

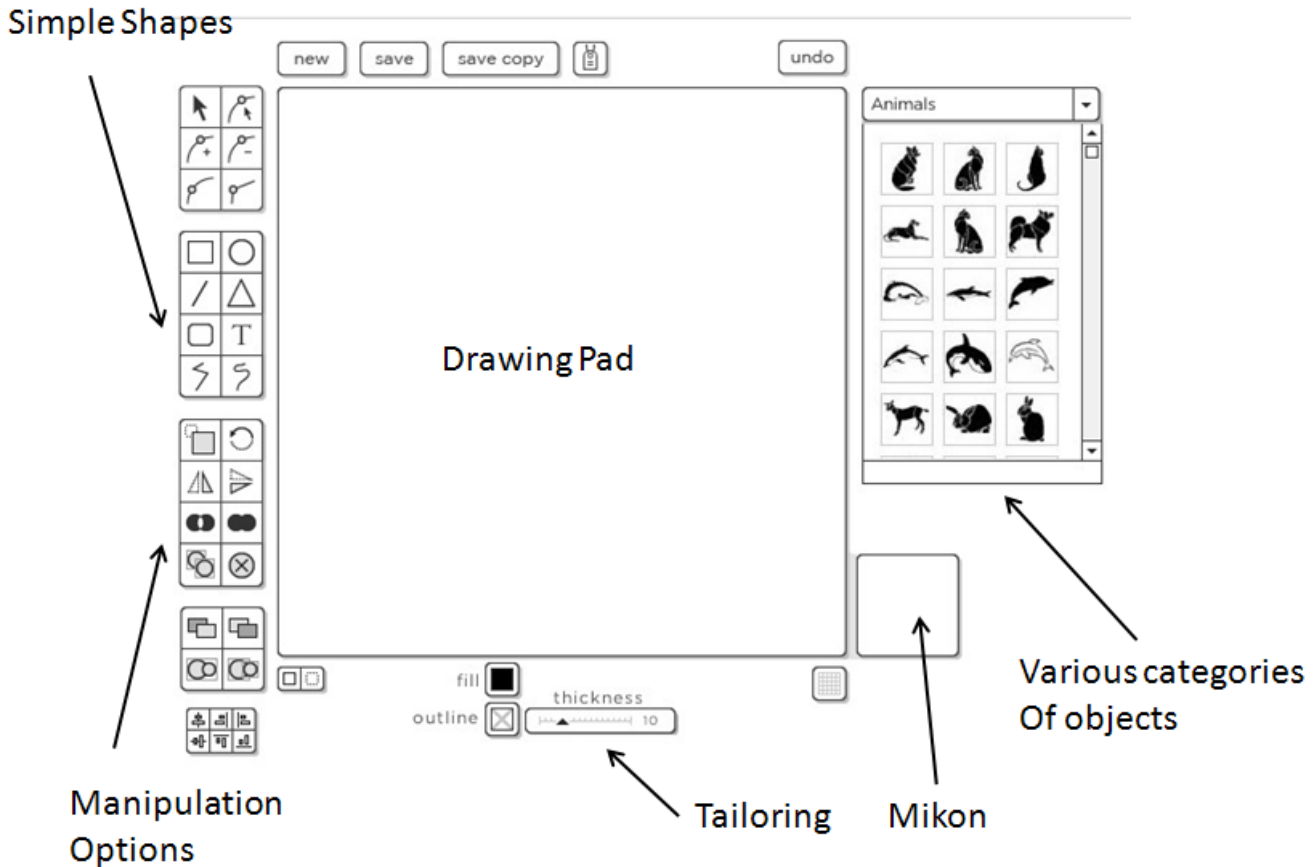


Fig. 2. Drawing Mikons

B. Authentication

During authentication, the pupil identifies him or herself by means of an email address. A screen then appears with four challenge sets displayed below each other, each with 16 images: one target and 15 distractors, as shown in Figure 5. The challenge sets are displayed below each other so that even fairly small screens, such as the ones used at the school, will be able to show an entire challenge set at the same time, something which is essential to support the person in finding the target. It is considered unwise to require horizontal scrolling, whereas vertical scrolling is natural and simple with the ubiquitous scrolling mouse.

The pupil needs to choose one image in each set to proceed to the next page. Feedback is provided as each choice is made. A red circle shows that a choice has not yet been made, as shown for sets 3 and 4 in Figure 5. Choices from sets one and two have been made as is shown by the circles displaying green. No indication of the actual choice made is given, since that would make it too easy for an observer to see the choices.

It is important to reiterate, at this stage, that the distractors are fixed for the challenge sets. This means that users who try to determine the identity of target image by refreshing the page will find their efforts frustrated since the pictures may change position but will not themselves change.

The button at the bottom of the page displays the legend: “Please Select a Mikon from Each Stage”, and is inactive until

a choice has been made from each of the challenge sets. When this happens, the legend changes to “Ready to Login” and the button is activated.

If the targets have been correctly identified, the pupil is allowed to access the system. If not, another attempt can be made.

In many authentication systems, the system will lock a user out after three incorrect attempts. The teacher advised against this in the case of this system because it would be too easy for pupils to lock other pupils’ accounts in the case of a grudge. Since the possibility of guessing the correct combination of Mikons is 1 in 65536, it was considered enough of a deterrent in this context to withstand break-in attempts from other pupils, so no lock-out was implemented.


C. Replacement

Any authentication system needs a replacement strategy. In this system the teacher could request that a pupil be allowed to redraw his or her Mikons if they were forgotten, by using the auxiliary teacher system. This meant the pupil could work through the registration process again, drawing a new set of Mikons, although in this case all homework details were retained.


IV. RESULTS

Twenty six pupils enrolled in February. The teacher entered a homework sheet into the system and they used the system


Stage 1 of 4 Select your Mikon from below




Stage 2 of 4 Select your Mikon from below



Stage 3 of 4 Select your Mikon from below



Stage 4 of 4 Select your Mikon from below



Please Select A Mikon From Each Stage

Ready To Login...

Fig. 5. Authenticating

during school in early March to complete the homework sheet.

In June another homework sheet was loaded and pupils were requested to complete it. Finally, in September a final homework sheet was posted for pupils to complete. The publication of this final sheet constituted a convenient mechanism for testing long-term memory of the Mikons.

A. Analysis based on logged attempts

From the first use of the system to the last, there were 134 authentication attempts by 24 pupils. An examination of the success and failure of each attempt indicates an 87% success rate. Eighteen of the pupils had a 100% success rate with 6 showing one or more failed attempts. Each of these pupils

successfully authenticated without problems during their last use of the system, which suggests that something unusual was occurring during the earlier attempts.

A closer examination of these attempts was conducted to ascertain what was happening. The 6 pupils with failed attempts fell naturally into one of three categories characterised by the pattern of successes and failures.

1) *Unexplained Pattern of Attempts*: One pupil fell into this category. He had 3 failed attempts followed by success. The attempts followed on directly from each other and it took 2 minutes from first to last. In each attempt the first 3 Mikons were chosen correctly, but a different incorrect Mikon was chosen in the fourth challenge set.

Six minutes later another unsuccessful attempt was registered by the system, followed by success 1 minute later. This pattern was repeated 18 minutes later.

The next attempt occurred yet 24 minutes later and was successful. The final attempt occurred in June and was, again, successful. With just this data it is impossible to draw reliable conclusions as to the reasons for the failures. It could be that a classmate was trying to guess the pupil's Mikons, but it could also be that the pupil himself was struggling, although the successful attempt in June suggests that this was not the case.

2) *Probable Intrusions*: The three pupils in this category have similar patterns: initial success, then one or more failures, followed by one or more successes (Fig 6). If these failed attempts are examined as a unit, their timestamps suggest an attack by one of the pupils' classmates. Each took place outside of school hours: one at 5:59pm and the others between 9:56pm and 10:10pm. The attempts incorrectly identified between 2 and 4 Mikons, varying choices between attempts. This strongly suggests that someone was attempting to intrude into these pupils' accounts.

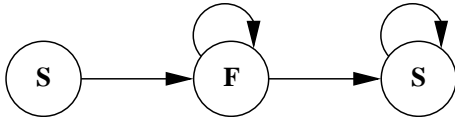


Fig. 6. Probable Intrusion (S=Success, F=Failure)

3) *Initial Problems then Success*: Two pupils fall into this category (Fig 7). The first chose an incorrect Mikon in the third challenge set, and corrected immediately thereafter. She had 7 subsequent successful authentications, which suggests that the first one was a slip.

The second pupil identified the same incorrect Mikon in the third challenge set during the first four attempts. After this, the pupil authenticated successfully. This was followed by four subsequent successful authentications, one of which took place in October — a full 8 months after the pupil initially drew the Mikons.

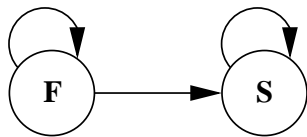


Fig. 7. Initial Problems Resolved (S=Success, F=Failure)

Examination of the second pupil's Mikons reveals the reason for the confusion. The target Mikon includes various images related to Halloween, but one of the distractors also has the same theme, even though the colours were different. This suggests that the pupil remembered drawing a Mikon based on the Halloween theme, and was confused by the similarity between the target Mikon and the distractor. The two Mikons are shown in Figure 8.

If one removes the probable intrusion attempts, the success rate of the Mikons system is 92%, which exceeds expectations and out-performs any password system [37], [38], especially where the system is used infrequently, which was the case here.



Fig. 8. Target Mikon (left), Distractor (right)

B. Analysis

Whereas failed attempts could well not be failed attempts but rather failed intrusions, successful authentications could equally be successful intrusions. Merely examining the records in the database gives a very superficial view of the viability of Mikons in graphical authentication. In order to gain a deeper understanding of the performance of the Mikons in this context, a final investigation was conducted which involved discussions with pupils and the teacher.

1) *Pupils*: A folder was constructed containing a number of sheets, each sheet displaying a different pupil's 4 Mikons. Sheets were labeled numerically to anonymise authorship. Each of the pupils was requested to indicate which were a) their Mikons and b) which sets of Mikons they could attribute to one of their classmates. The first question would indicate memorability while the second would indicate how easy it was to link the Mikons to the author.

All pupils immediately identified their own set of Mikons without any difficulty or hesitation. This is a strong confirmation of the superior memorability of Mikons.

Pupils were asked to identify other Mikons' creators. Some pupils declined to hazard a guess but some pupils thought they could identify authors. Only 4 pupils out of the 27 questioned correctly identified the creator of another set of Mikons. The successful guessing rate was therefore 15%. There are some factors which need to be considered when judging this success rate: the pupils all drew their Mikons during the same lesson and could easily have observed each other while they were drawing. The pupils also, as mentioned before, know each other very well, and can make accurate guesses about the kinds of drawings other pupils would be likely to produce. Finally, by presenting the Mikons without their distractors, it was much easier for them to make an educated guess about the artist's identity based on knowledge of only one of the Mikons in the set. For example, if a pupil knew *one* of the other pupil's mikons, then the artist was identified. If the pupil's Mikons had been presented as part of the challenge set, they would not know whether the Mikon they "knew" was the target or a distractor, and would find it far more challenging to correctly identify the other three Mikons and be able to break into the other pupil's account.

Even if we accept that these factors make guessing other pupils' Mikons particularly likely to succeed, the fact remains that Mikons might well be too predictable to control access to sensitive or valuable data. However, there are many low

risk systems currently using passwords which could benefit from the superior memorability of the Mikons. It is vital that the strength of the authentication mechanism matches both the risk level of the asset being protected and the abilities of the users [39]. For a system such as the online homework system, the Mikon strengths in the context of graphical authentication might well outweigh this level of predictability.

2) *Teacher*: The teacher was very enthusiastic about the use of Mikons in authenticating the pupils. She noted that the system was better than the password system because she did not have to spend any time resetting passwords at the beginning of each lesson. She also noticed that pupils were not as prone to share information about their Mikons as they were to divulge their other passwords because they were harder to describe. Pupils would often share passwords with their best friends and when the friendship turned sour the ex-friend would share the password with many other pupils, necessitating a password reset. She also observed that some pupils, after a time lapse of a few months, thought that they would not remember their Mikons but when they accessed the system they had no difficulty identifying them from the challenge sets.

The teacher did not mind approving the pupils' Mikons, indeed she considered that a part of her job. Furthermore, no pupils requested a Mikon "password" reset or distractor changes, so concerns about the burden placed on the teacher were unfounded.

From the teacher's point of view the Mikon-based graphical authentication system was a very satisfactory authentication mechanism which met the accessibility requirements.

V. DISCUSSION

This longitudinal experiment was conducted in order to determine how well Mikons would perform in authenticating a group of users with widely ranging developmental levels and language skills. The results will be discussed in terms of memorability, predictability and scalability.

Memorability: The literature related to memorability of drawn images suggested that Mikons would be memorable, and this proved to be the case. All pupils unhesitatingly identified their own Mikons, even after a seven to eight month lapse.

Predictability: In terms of predictability, Mikons did not perform as well as hoped although, in this setting, they certainly performed much better than the weak passwords used by this user group. Certainly with the potential for intelligent password guessing in this group, Mikons offers a more secure alternative. It should be noted that the testing of Mikons in this context is a particularly stringent test. These pupils know each other very well and are more likely to be able to predict the kinds of Mikons that will be drawn by other pupils. There is also a strong possibility that the pupils observed each other drawing their Mikons. Finally, as mentioned before, in order for Mikons to be effective in authentication, the person drawing the Mikons needs to exercise a measure of dissemination, anticipating what other users may guess that they will draw, and doing something different. It is possible

that the users of the Mikons-based system were not yet able to disseminate successfully or did not sufficiently understand security requirements to understand the need for it.

Furthermore, they are at an age where they are likely to experiment and attack the system, just to see whether they can do it. There is evidence that one or more pupils *did* attempt to attack the system, and at least some of the attacks were resisted. It is impossible to know how many succeeded.

Scalability: Mikon authentication, as is the case with any system which allows users to upload content, requires a measure of human involvement in order to curb the activities of the less well behaved users of the system. It should be borne in mind, however, that the incidence of forgotten passwords will drastically reduce, which means that fewer resources need to be deployed in resetting passwords. Moreover, the time required to approve the drawn Mikon images is a one-off cost, incurred at enrolment, unlike password resets which can occur at any time throughout the user's use of the system.

The use of Mikons in authentication was tested to provide an accessible and viable alternative to drawings (in terms of scalability) and passwords (in terms of accessibility). Mikons definitely support a more scalable system than do drawings, which have to be manually scanned and uploaded. They also have high memorability and are more widely accessible than traditional passwords.

Their predictability could be a problem for systems with higher security requirements, but for this system the Mikons provided exactly the right balance between security, memorability and accessibility.

As explained in Section III, the authentication requirement for the online homework system was a fairly relaxed one. It was vital that the pupils should be able to access the system and a more stringent authenticator, such as a password, would deliver a level of security beyond that which was required in this context.

VI. FUTURE WORK

This study had a relatively small sample size, and this is a limitation which needs to be acknowledged. However, the findings of this study have shown that Mikons have the potential to justify a larger and more substantial study. Such a study would ideally include a wider range of ages, disabilities and abilities as well as a larger number of participants.

The follow-up investigation which was conducted, with respect to artist attribution, suggests a number of other avenues for investigation. It would be interesting to see whether the teacher could attribute Mikons to the artists, or perhaps whether an uninvolved outsider could guess at the gender or age of the artist. This would help us to assess the likelihood of an outsider attack succeeding, rather than the insider attack focused on in this investigation.

VII. CONCLUSION

This paper reported on a longitudinal experiment to assess the viability of Mikons in authenticating a group of users with a wide range of developmental and language skills. The system in question, an online homework system, required

a knowledge-based authenticator where the balance between security and memorability was tipped to memorability, with security being slightly less important than is usual with other, higher-risk systems.

Mikons proved their superior memorability, as predicted by the literature and confirmed by discussions with the pupils themselves. Enrolling the pupils was also relatively simple with many of the processes being automated, meaning that in terms of scalability Mikons performed well. The Mikons were somewhat predictable, but in terms of security they proved to be a *necessary and sufficient* authenticator within this context. This was particularly important with this system's target user group and the Mikon authenticator accommodated the variety of skills and abilities of the users for whom yet another password would have been an unjustified burden.

ACKNOWLEDGMENTS

I am very grateful to the mikons.com company for permission to use their Mikon engine in this research. A special note of thanks to Mark Smith at mikons.com, my primary contact at the company.

I would also like to thank the anonymous reviewers for their helpful and constructive comments.

REFERENCES

- [1] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," *Commun. ACM*, vol. 47, no. 4, pp. 75–78, 2004.
- [2] A. Sasse and I. Flechais, "Usable security: Why do we need it? How do we get it?" in *Security and Usability*, L. Cranor and S. Garfinkel, Eds. O'Reilly, 2005, ch. 2.
- [3] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "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*, vol. 63, no. 1-2, pp. 128–152, July 2005.
- [4] M. Eagle and E. Leiter, "Recall and recognition in intentional and incidental learning," *Journal of Experimental Psychology*, vol. 68, pp. 58 – 63, 1964.
- [5] S. Madigan, "Picture memory," in *Imagery, memory, and cognition: essays in honor of Allan Paivio*, J. Yuille, Ed. Hillsdale, NJ: Lawrence Erlbaum Associates, 1983, pp. 43–69.
- [6] R. N. Shepard, "Recognition memory for words, sentences and pictures," *Journal of Verbal Learning and Verbal Memory*, vol. 6, pp. 156–63, 1967.
- [7] L. Standing, "Learning 1000 pictures," *Quarterly Journal of Experimental Psychology*, vol. 25, pp. 207–222, 1970.
- [8] A. Paivio, *Mental representations: A dual coding approach*. Oxford, UK: Oxford University Press, 1986.
- [9] D. Katre, "Using mnemonic techniques as part of pictorial interface for self-identification of illiterate villagers," in *Proc I-HCI 2004*, Bangalore, India, 6-7 Dec 2004, <http://www.cdac.in/html/pdf/dkatre.pdf>. Accessed: October 2008.
- [10] A. Schmidt, T. Kölbl, S. Wagner, and W. Strassmeier, "Enabling access to computers for people with poor reading skills," in *8th ERCIM Workshop on User Interfaces for All. Lecture Notes in Computer Science (LNCS)*, Vol. 3196, C. Stary and C. Stephanidis, Eds., Vienna, Austria, 2004, pp. 96–115.
- [11] T. Mendori, M. Kubouchi, M. Okada, and A. Shimizu, "Password input interface for primary school children," in *Proceedings of the International Conference on Computers in Education (ICCE02)*, Auckland, New Zealand, December 3-6 2002, pp. 765–766.
- [12] K. Renaud, "A visuo-biometric authenticaton mechanism for older users," in *Proc British HCI 2005. Sept 5-9, Edinburgh*, 2005, pp. 167–182.
- [13] —, "On user involvement in production of images used in visual authentication," *Journal of Visual Languages and Computing*, no. 1, pp. 1–15, 2009.
- [14] T. S. Tullis and D. P. Tedesco, "Using personal photos as pictorial passwords," in *CHI2005*, Portland, OR, USA, 2005, pp. 1841–1844.
- [15] T. Pering, M. Sundar, J. Light, and R. Want, "Photographic authentication through untrusted terminals," *Security & Privacy*, vol. 2, no. 1, pp. 30–36, 2003.
- [16] J.-H. Lim, Q. Tian, and P. Mulhem, "Home photo content modeling for personalized event-based retrieval," *IEEE Multimedia*, vol. 10, no. 4, pp. 28–37, 2003.
- [17] R. Dhamija and A. Perrig, "D'jà vu: A user study using images for authentication," in *Proceedings of USENIX Security Symposium*, Denver, Colorado, August 2000, pp. 45–58.
- [18] P. Dixon and S. Glover, "Action and memory," in *The Psychology of Learning and Motivation*, B. H. Ross, Ed. Academic Press, 2004, pp. 143–174.
- [19] H. D. Zimmer and R. L. Cohen, "Remembering actions: A specific type of memory," in [40], 2001, pp. 3–24.
- [20] H. D. Zimmer, "Why do actions speak louder than words? Action memory as a variant of encoding manipulations or the result of a special memory system?" in [40], 2001, pp. 151–197.
- [21] J. Engelkamp, H. D. Zimmer, G. Mohr, and O. Sellen, "Memory of self-performed tasks: self-performing during recognition." *Memory & Cognition*, vol. 22, no. 1, pp. 34–9, Jan 1994.
- [22] A. Koriat, H. Ben-Zur, and A. Nussbaum, "Encoding information for future action: Memory for to-be-performed tasks versus memory for to-be-recalled tasks," *Memory & Cognition*, vol. 18, no. 6, pp. 568–578, 1990.
- [23] L. Nyberg and L.-G. Nilsson, "Recall of actions, sentences and nouns. influences of adult age and passage of time," *Acta Psychologica*, vol. 79, pp. 245–254, 1992.
- [24] M. Knopf, A. Mack, A. Lenel, and S. Ferrante, "Memory for action events: Findings in neurological patients," *Scandinavian Journal of Psychology*, vol. 46, pp. 11–19, 2005.
- [25] G. Knoblich and W. Prinz, "Recognition of self-generated actions from kinematic displays of drawing," *Journal of Experimental Psychology: Human Perception and Performance*, vol. 27, pp. 456–465, 2001.
- [26] P. A. Leynes, J. A. Grey, and J. T. Crawford, "Event-related potential (ERP) evidence for sensory-based action memories," *International Journal of Psychophysiology*, vol. 62, pp. 193–202, 2006.
- [27] M. Longcamp, J. L. Anton, M. Roth, and J. L. Velay, "Visual presentation of single letters activates a premotor area involved in writing," *Neuroimage*, vol. 19, no. 4, pp. 1492–500, aug 2003.
- [28] B. H. Repp and G. Knoblich, "Perceiving action identity: How pianists recognize their own performances," *Psychological Science*, vol. 15, no. 9, pp. 604–9, 2004.
- [29] R. Flach, G. Knoblich, and W. Prinz, "Recognising one's own clapping: The role of temporal cues," *Psychological Research*, vol. 69, pp. 147–156, 2004.
- [30] F. Loula, S. Prasad, K. Harber, and M. Shiffrar, "Recognizing people from their movement," *Journal of Experimental Psychology*, vol. 31, no. 1, pp. 210–220, 2005.
- [31] M. E. Foley and H. H. Ratner, "The role of action-based structures in activity memory," in [40], 2001, ch. 5, pp. 112–135.
- [32] J. Andrade, "What Does Doodling Do?" *Applied Cognitive Psychology*, 2009, to Appear.
- [33] J. Engelkamp and H. D. Zimmer, "Similarity of movement in recognition of self-performed tasks and of verbal tasks," *British Journal of Psychology*, vol. 86, pp. 241–252, 1995.
- [34] M. Sturken and L. Cartwright, *Practices of Looking: An Introduction to Visual Culture*. Oxford University Press, 2001.
- [35] P. N. Mathur, "Barriers to effective visual communication," *Media Asia*, vol. 3, pp. 160–4, 1978.
- [36] R. Poet and K. Renaud, "A mechanism for filtering distractors for graphical passwords," in *13th Conference of the International Graphonomics Society Melbourne, Australia. 11-14 November, 2007*, pp. 129–132.
- [37] J. Bunnell, J. Podd, R. Henderson, R. Napier, and J. Kennedy-Moffat, "Cognitive, associative and conventional passwords: Recall and guessing rates," *Computers & Security*, vol. 16, no. 7, pp. 629–641, 1997.
- [38] A. S. Brown, E. Bracken, S. Zoccoli, and K. Douglas, "Generating and remembering passwords," *Applied Cognitive Psychology*, vol. 18, no. 6, pp. 641 – 651, 2004.
- [39] K. Renaud, "A process for supporting risk-aware web authentication mechanism choice," *Reliability Engineering and System Safety, Special Edition*, vol. 92, no. 9, pp. 1204–1217, 2007.
- [40] H. D. Zimmer, R. L. Cohen, M. J. Guynn, J. Engelkamp, R. Kormi-Nouri, and M. A. Foley, Eds., *Memory for Action. A Distinct Form of Episodic Memory*. Oxford University Press, 2001.