PassShapes - Utilizing Stroke Based Authentication to Increase Password Memorability

Roman Weiss
Media Informatics Group
University of Munich
Amalienstr. 17
80333 Munich, Germany
weissr@cip.ifi.lmu.de

Alexander De Luca
Media Informatics Group
University of Munich
Amalienstr. 17
80333 Munich, Germany
alexander.de.luca@ifi.lmu.de

ABSTRACT
Authentication today mostly relies on passwords or personal identification numbers (PINs). Therefore the average user has to remember an increasing amount of PINs and passwords. Unfortunately, humans have limited capabilities for remembering abstract alphanumeric sequences. Thus, many people either forget them or use very simple ones, which implies several security risks. In this work, a novel authentication method called PassShapes is presented. In this system users authenticate themselves to a computing system by drawing simple geometric shapes constructed of an arbitrary combination of eight different strokes. We argue that using such shapes will allow more complex and thus more secure authentication tokens with a lower cognitive load and higher memorability. To prove these assumptions, two user studies have been conducted. The memorability evaluation showed that the PassShapes concept is able to increase the memorability when users can practice the PassShapes several times. This effect is even increasing over time. Additionally, a prototype was implemented to conduct a usability study. The results of both studies indicate that the PassShapes approach is able to provide a usable and memorable authentication method.

Categories and Subject Descriptors
D.4.6 [**Operating Systems**]: Security and Protection – *access controls, authentication;* K.4.4 [**Computers and Society**]: Electronic Commerce – *security;* K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *authentication.*

General Terms
Experimentation, Security, Human Factors.

NordiCHI 2008: Using Bridges, 18-22 October , Lund, Sweden.

Keywords
Authentication, Security, Shape Passwords, Graphical Authentication, PassShapes.

1. INTRODUCTION
User authentication is an important issue in using computer systems since ever. The resources and services offered by the systems have to be protected against unauthorized access. Today most systems use alphanumeric passwords or *Personal Identification Numbers* (PINs) as authentication tokens. Due to the emerging ubiquity of computing and the vast amount of used services and devices the average user has to keep an increasing number of passwords and PINs in memory these days. Authentication is not only required by the computer systems at home or at the office, today even garage doors ask for a PIN. We carry mobile phones, PDAs which are protected by PINs and we use plenty of public terminals and online services that demand authentication. From ATMs for withdrawing money, point-of-sale terminals for paying in a store or when logging on to personalized websites, passwords and PINs have widely spread in our everyday lives.

But these passwords and PINs have well-known deficiencies. The main problem is that they always state a compromise between memorability and security. For security issues a password should be composed of a long and random sequence of characters with high entropy. Unfortunately the human brain struggles in memorizing such meaningless and random strings. So users tend to use short, simple and meaningful passwords, what increases the probability that these passwords can be guessed or revealed by a dictionary attack. In fact studies made over the last 30 years show that many of the used passwords can be compromised easily. For example Klein shows already 1990 that he could crack 25% of 14000 passwords using a dictionary consisting of only 86000 words [12]. This is why the user is often referred to as the 'weakest link' in the security chain [20]. According to this, in a study regarding PINs we found out that over 40% of the participants stated 'yes' when asked if they used simple ones like birthdays,

'0000' or the like. On the other hand, if complex passwords have to be used, users tend to forget them. In our study almost everyone stated that he had already forgotten a password and almost 80% had to admit that they had already forgotten a PIN.

One might argue that using biometric methods might solve these problems best since they can prove the identity of a person without having the user to remember anything. But the application of biometric methods bears its own specific problems. Biometric data is very sensitive as it enables to identify a person unambiguously. Many persons may have privacy concerns when providing biometric data to service providers or employers. Having a fingerprint stored in the databases of web shops will surely cause many users' worries, as the security of the stored data is important for both security and privacy of the users of a biometric system. Another problem comes along with the uniqueness of biometric features: when it is once possible to forge such a biometric feature, this results in severe problems for the authentication system. The recent successes of German hackers in forging fingerprints with simple do-it-yourself products like glue and graphite are indeed alarming. Due to these problems knowledge-based authentication systems are not to be outdated in the near future.

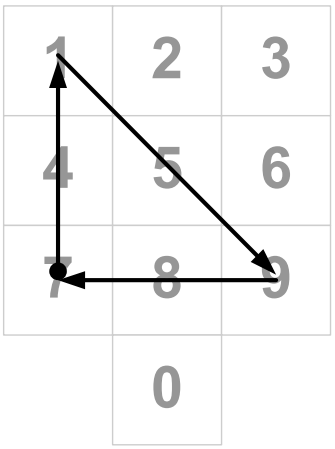

Figure 1: A shape used to remember the PIN 7-1-9-7

In this work we try to show ways to overcome problems regarding memorability and provide an approach for a novel knowledge-based authentication system. In previous work [7] we evaluated different authentication techniques for ATM usage. During the experimentations we found that many users tend to support their memory for their 4-digit-PINs by incorporating the layout of the digits on the number pad and the shape resulting from these spatial relations. Figure 1 shows an example: when entering the PIN 7197 a triangle is made on the number pad. This shape is used by many users to support their memory. In a conducted user study over 40% of the participants stated that they use this mnemonic for memorizing PINs.

This finding motivated the development of the PassShapes concept introduced in this paper. This concept uses simple, stroke-based drawings for authentication instead of numeric or alphanumeric sequences.

We argue that the PassShapes approach that will be outlined in detail in the next section will offer better memorability than today's password- or PIN-based systems. Research from various academic disciplines like cognitive psychology and neurosciences supports that theory which will be explained in section 3. Section 4 presents the results from the conducted user studies regarding the memorability and the usability of the presented approach. Afterwards the PassShapes concept is compared to other concepts dealing with graphical authentication considering the security and the usability of the different systems. The paper closes with a conclusion and an outlook to future work.

2. THE PASSSHAPES CONCEPT

The concept developed in this work is based on the observation that users utilize shapes when entering PIN numbers for supporting their memory as depicted in Figure 1. The idea is, if users mostly remember the shape and not the corresponding PIN, why not getting rid of the numbers completely? Therefore, in the PassShapes concept we now eliminate PINs as authentication tokens and use such simple geometric shapes instead. These PassShapes are composed of strokes. There are eight different possible strokes defined which are illustrated in Figure 2.

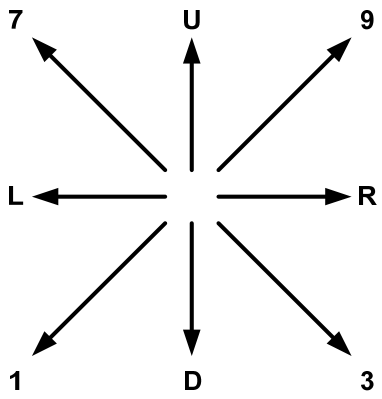

Figure 2: The eight different strokes used in the PassShapes concept

Several strokes consecutively drawn without lifting the pen are called a stroke sequence. A PassShape itself may consist of several stroke sequences, that is, several disconnected shapes as seen in Figure 3. PassShapes can be represented by an alphanumeric string for internal processing and storage. Each stroke has a corresponding character representation as depicted in Figure 2, where the letters indicate the stroke directions: an 'L' stands for 'left',

an ‘R’ stands for right etc. whereas the numbers refer to the direction equivalent to the position of the number on a standard number pad (i.e. ‘7’ corresponds to ‘top left’). A pen-up event separating two stroke sequences is marked with an ‘X’. Figure 3 shows an example PassShape consisting of two stroke sequences and eleven strokes in total.

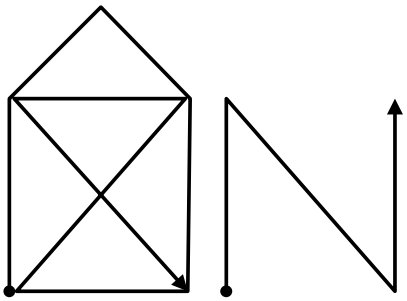

Figure 3: An example PassShape with the internal representation U93DL9L3XU3U

For authentication the user has to reproduce his PassShape either using a touch screen, touch pad or another pointing device. The important aspect is that the strokes of a PassShape are always drawn in the same order, which additionally supports memorability as explained later. Additionally, it is not necessary to redraw a PassShape in exactly the same size or position, since only the strokes and their order are evaluated.

PassShapes solely consist of straight lines and so painting is easy and effortless even for non-artistic users. In the next section we will try to affirm the assertion that geometric forms like the just described PassShapes will provide a better memorability than classic passwords and PINs.

3. PASSSHAPE MEMORABILITY

The expected enhanced memorability of PassShapes is supported by various functionalities of the human brain. First of all, humans have extensive capabilities in remembering pictures. This is called the *pictorial superiority effect* and is proven empirically in many experiments made by cognitive psychologists since the late 1960s. Image processing and image memory is still a challenge to scientists as theories covering these aspects satisfactory still lack, but the existence of the *pictorial superiority effect* is beyond dispute. See Standing’s work for pictorial superiority for recognition memory [22] or Paivios’s work for the superiority of pictures regarding free recall [17]. As PassShapes are pictorial stimuli we can expect a better memory performance caused by the *pictorial superiority effect*.

Another particularity of PassShapes is the fact that they are drawn by hand. This enables the processing and storage of the PassShape as a motor scheme in the procedural memory. The procedural memory is the counterpart to the declarative memory, where facts and knowledge are processed and stored. The motor memory is amongst other things a part of the procedural memory and responsible for the coding and storage of motor schemes. The usage of the motor memory for memorizing PassShapes has some advantages: First, the motor memory is very powerful. Once learnt motor schemes can easily be accessed even after they have not been used for months, as shown by Shadmehr and Brashers-Krug in [21]. Furthermore, the motor memory can be trained by simple repetition. This enables us to provide a simple but effective strategy for memorizing PassShapes. Simple repeated drawing of the PassShape supports the storage of a specific motor scheme in the procedural memory. Research by Naka et al. [14] investigating this effect clearly shows that especially for geometric forms repeated drawing is involving significant improvements of memory performance. Conventional passwords and PINs can only be stored in the declarative part of the memory. Here simple repetition is very ineffective. To provide a good consolidation of such declarative information it has to be processed and linked to existing memory schemata. Therefore, a high “depth of processing” is necessary. This term, introduced by Craik and Lockhart, expresses that it is important to execute as many operations and build as many associations with new information as possible to achieve a good memory performance [4]. But this can be difficult when random-like numbers and meaningless strings must be processed. With PassShapes the building of associations and operations can be easier. Due to the simplicity of the PassShapes and their graphic presentation the identification of triangles, squares and roofs or other distinctive features like symmetry or similarities to real-world objects can help to achieve a higher depth of processing and thus a better consolidation in memory.

The fact that PassShapes have a fixed stroke order is also helping our memory. This can be derived from research investigating the learning of Chinese characters. Chinese characters also consist of strokes and can thus be regarded as functionally similar to PassShapes. When writing these characters a strict stroke order has to be followed. The findings of Flores d’Arcais [11] show that the fixed stroke order is an important help for learning and memorizing the characters.

There is strong evidence that due to their graphic nature and due to the involvement of motor memory PassShapes could provide better memorability compared to today’s passwords and PINs. In the next section a user study is described, which has been performed to examine this assertion.

4. USER STUDIES

We conducted several user studies in order to prove the claimed theoretical advantages and to find out if the

proposed PassShapes will have the potential to establish themselves as an alternative authentication method. Therefore, for both evaluations, standard PIN entry has been used for comparison

4.1 User study 1: Memorability

The main study of this work has been performed to investigate the memorability of PassShapes.

User Study Design

For the memorability evaluation, a repeated measures inter-subject longitudinal experimental design was used. This way, it was possible to measure the memory effect of PassShapes over a longer period of time. Three different groups were created to evaluate and compare three different combinations of the independent variables *method* (seven-stroke PassShapes, five-digit PINs) and *strategy* (none, repeated drawing). The combinations were PIN + none, PassShapes + none and PassShapes + repeated drawing.

The decision not to test PIN + repeated drawing was made since drawing PINs in order to stimulate the motor memory is not the common way to use PINs. Usually they are input using buttons on keyboards, keypads, mobile phones and the like. That is, the goal was to compare PassShapes to standard PINs.

PassShapes consisting of seven strokes were chosen because there exist more than 100,000 different PassShapes of this class, which corresponds to the complexity (password space) of five-digit PINs.

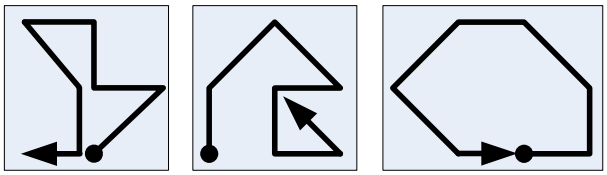

Figure 4: Example PassShapes used in the user study

Hypothesis

With respect to the scientific work performed in the sector of memorability of pictures, motor memory and the like as mentioned before, our hypotheses for the memorability study were:

(H1) PassShapes will be easier to remember than PINs.

(H2) PassShapes using repeated drawing will be easier to remember than PassShapes without the repeated writing memory strategy and PINs.

Participants

For the study, 52 volunteering participants were randomly assigned to three experimental groups. The average age of the subjects was 34.5 years. The youngest participant was 22 years old, the oldest 63. 46% were female. 77% held a university entry diploma and 60% an academic degree. There were no significant differences between the three groups regarding demographic data like age, sex and education.

Procedure

The first group was used as reference group and was handed out five-digit PINs created with a random generator tool. The subjects were told to try to memorize the PIN. Afterwards, a survey collected demographic data and data concerning the usage of PINs in the participants' daily lives.

Subjects in the other two groups were given PassShapes constructed out of seven strokes. Figure 4 shows some example PassShapes used in the study. As the PINs, they were created with a random PassShape generator implemented in conjunction with this work.

In the second group the subjects were told to memorize the PassShapes (of course considering the correct stroke order), but no special strategy was communicated to them. In the third group the strategy outlined before utilizing the motor memory was investigated: the subjects had to repeat their PassShape 24 times. The experimenter was responsible for checking whether the correct stroke order was met. Afterwards the participants had to fill out the questionnaires collecting demographic data and data concerning common behavior related to PIN usage.

Besides collecting basic information, the questionnaire also had the purpose to distract the participants from their tasks and deleting their short term memory. Afterwards, the participants were asked to repeat the PINs and PassShapes. So it was measured how many participants could still remember their authentication tokens. This procedure was iterated after five and ten days. Whenever participants failed to reproduce their PassShape or PIN, they were presented it and told to try to remember it again. Participants in the third group that had forgotten their PassShape had to practice it again for 24 times (repeated drawing).

Results

The results of the memorability evaluation are listed and illustrated in Table 1 and Figure 5. They show the numbers of correct PINs and PassShapes in the three tests during the study for each of the three groups.

In the first test taken immediately after the learning phase, the PIN group and the PassShapes repeated drawing group showed 100% memorability rate, while PassShapes without strategy performed worse as 4 people had forgotten their PassShape. After 5 days, the PIN group still performed good with only one participant that had failed in remembering his number, while in the PassShape group 6 and in the PassShape group with repeated drawing 4 participants had forgotten their shape. After ten days the condition represented by group three, PassShapes

combined with the repeated drawing strategy showed the best results with over 94% correctly reproduced PassShapes. While the results of the PIN group and the PassShape group declined over time, the PassShape group with repeated drawing showed better results after ten days than after five days.

	Test 1	Test 2	Test 3
PIN	16/16	15/16	13/16
PassShapes	15/19	13/19	12/19
PassShapes with repeated drawing	17/17	13/17	16/17

Table 1: Number of correct answers in the different groups for the single tests

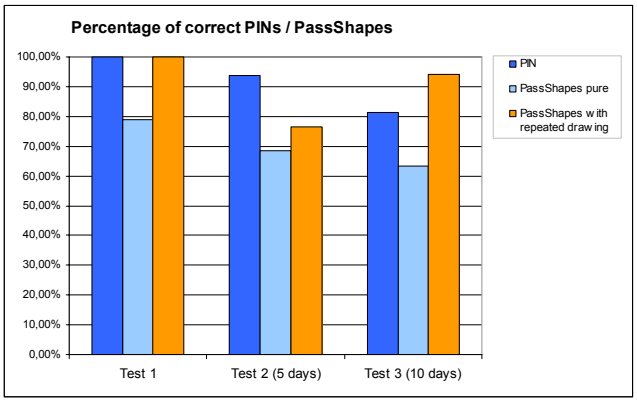

Figure 5: Percentages of correct PINs and PassShapes for the single tests

In the questionnaires we asked the subjects what strategies they utilized to memorize the PINs or PassShapes. The subjects in the PIN group all stated that they had used some kind of mnemonic for supporting their memory. And they were stunningly successful in creating these mnemonics. The users were able to construct very creative tricks: one user memorized the PIN 38714 with the following memory hook: "2 times 14 is not 38, but 2 times 7 is 14".

The behavior in the two PassShape groups was very different. In the group where the repeated drawing strategy was utilized 94% of the participants stated that they used auxiliary constructs for supporting their memory. Many identified triangles and other simple geometric forms in the PassShapes, others used symmetry or spatial relations of the PassShapes and yet others used associations regarding the total appearance of the PassShape. Examples for such associations are shown in Figure 6. Half of the users in the third group stated that they had explicitly used the drawing movement as a memory aid.

In the second group where no specific strategy was utilized by the subjects only 58% stated that they used some mnemonic for supporting their memory. Only 16% stated that the movement made by drawing could help memorizing the PassShapes.

Discussion

In contrast to hypothesis (H1), at the first glance, the results indicate that PassShapes without repeated drawing seem not to be more memorable than PINs. After talks with the participants and evaluating the questionnaires, the reason for these results became obvious. People are used to interacting with computer systems using PINs every day. Therefore, they are highly trained to develop and use strategies to remember them. As a result very effective memory hooks have been used even though the PINs were created randomly and seldom showed obvious regularities. This effect is possibly increased by the fact, that the participants in the study have a rather high educational level.

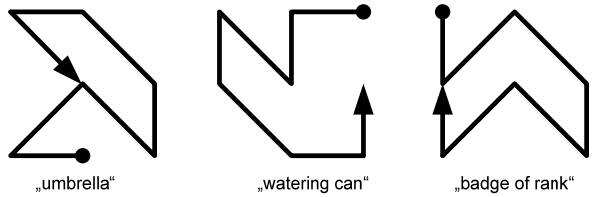

Figure 6: PassShapes and users' associations

Even though the result shows no statistical significance (α=0,075), they show that PassShapes – especially when combined with the repeated drawing strategy – can provide a very memorable authentication token. The assumption that practicing the PassShapes by drawing them repeatedly will cause a better memory performance as stated in hypothesis (H2) can be confirmed. With regard to the fact, that the efficient PIN strategies of the participants outperformed the pure PassShapes, this result is even more surprising. It shows that even without learned and practiced strategies the participants could easily remember them. The results indicate that the advantage of PassShapes is even increasing over time. This confirms the appropriateness of the utilization of motor memory for authentication tasks.

We can see that the subjects that used the repeated drawing strategy constructed significantly more memory aids than the others. They stated that they had identified simple shapes like triangles or squares, or used the spatial layout or the movement made while drawing to support their memory. With the theory introduced in section three this can be explained with a higher depth of processing. The repeated reproducing of the PassShape and the resulting intense occupation with it supports the consolidation process, leads to a better processing and storage and thus increases the declarative memory performance. Additionally, the motor scheme created by the repeated drawing can be stored in the procedural memory. Using PassShapes together with the repeated drawing mnemonic strategy leads to a dual storage of the information. Both declarative and procedural memory are involved and

activated. As these different functions of the human memory are also located in different physiologic parts of the brain it is reasonable to assume that this simultaneous storage can have a positive effect on the overall memory performance.

In this study we could collect insights that indicate that PassShapes are indeed very memorable especially when the repeated drawing strategy is used.

4.2 User study 2: Usability

Knowing that an authentication method is easy to remember still does not qualify it as an appropriate interaction method. Thus it was necessary to conduct a user study on the performance of the PassShapes concept regarding user convenience. As authentication is occurring very often in our daily lives it is important that the authentication process can be executed fast and effortless. Also very important for the authentication with PassShapes is a robust detection of the drawn PassShapes. A PassShape detection algorithm should recognize as many PassShapes as possible – regardless the artistic talent of the single user. In order to find out the capabilities of the new approach a user study considering the usability was conducted.

Figure 7: A user performing a task during the study.

User Study Design

For the usability evaluation, an intra-subject factorial design has been chosen. The independent variables were *method* (seven-stroke PassShapes and five-digit PINs) and *task* (log-on, change password). Therewith, the two most common tasks regarding authentication have been chosen. Therefore, each participant had to perform four sets during the user study (*method* x *task* = 4). The order of the sets was evenly distributed amongst the participants.

The dependent variables measured in the experiment were *input errors* and *time*.

Additionally, following the think-aloud technique, the participants were asked to speak out what they are thinking while performing the interaction.

Hypothesis

For the usability study, two hypotheses regarding the error rate and interaction speed were stated:

(H3) Due to their common usage, entering PINs will be slightly faster than entering PassShapes, but PassShape performance times will be acceptable.

(H4) The participants will not have any major problems performing the tasks with PassShapes and thus the error rate will be low.

Participants

The study has been performed with twelve participants with an average age of 29. Half of the participants were female. The youngest participant was 27 years old, while the oldest one was 30 years.

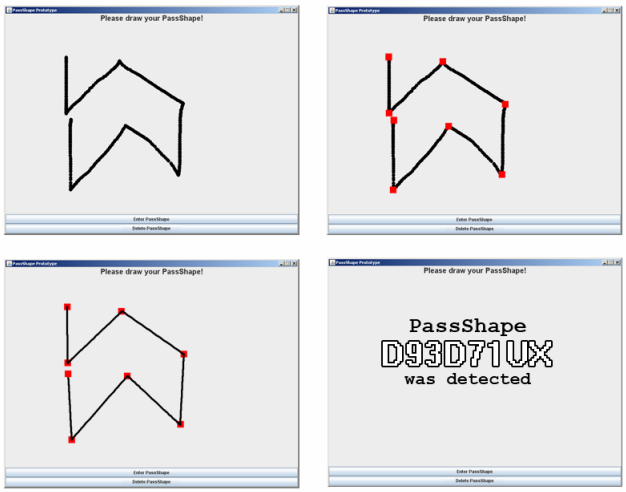

Figure 8: top left: the user-drawn PassShape; top-right: the extraction of the edges; bottom-left: stroke-detection with the edges; bottom-right: internal representation of the detected PassShape

Procedure

Every participant had to complete the previously mentioned four sets of interaction. The first set was a normal log-on process. The PIN had to be entered and the PassShape had to be drawn, respectively. The second task was a 'change-password'-task: at first the 'old' PIN or PassShape had to be entered and then the 'new' ones had to be entered twice, as usual, for confirmation. The time needed for entering was measured and the input errors were counted. Again five-digit PINs and seven-stroke PassShapes were used. Figure 7 shows a user performing a task with the prototype.

Prototype

To conduct this study a prototype was implemented in Java. It was set up on a Tablet-PC with a capacitive touch screen. A stylus was used to draw the PassShapes. The implemented algorithm tried to extract the edges of the

drawing during input. Therefore the speed and the acceleration of the stylus were analyzed. As PassShapes cannot contain circles, ellipses or arcs the position of the edges allows an exact detection of the drawn strokes. Figure 8 illustrates the detection process: While the user draws the edges are extracted. With the position of the edges the drawn strokes can be calculated and thus the PassShape can be reproduced. In the end the strokes are translated to the internal representation for further processing.

The prototype itself has only two command buttons. One for deleting the input and one for finishing input. The prototype used for the PIN-entry tasks was a simple number pad displayed on a touch screen.

Results

The average input time for a PIN was 4.2 seconds (SD=1.3s). This is faster than the average input time for a PassShape with 6.5 seconds (SD=2.0s). A t-test shows significance of the result that the PIN-entry is faster than the PassShape entry (t=3,36, df=22, p<0,003). The second task showed similar results: Changing a PIN took an average of 14.6 second (SD=3.1s) whereas changing a PassShape took 19.5 seconds (SD=5.5s). This result is also statistically significant (t=2,71, df=22, p<0,02). The results are summarized in Table 2.

The error rates were very low in all the cases, while the error rate for PassShapes was slightly higher.

	Logging on	**Changing password**
PINs	4.2 sec	14.6 sec
PassShapes	6.5 sec	19.5 sec

Table 2: Interaction times for PINs and PassShapes for the two different tasks

Discussion

This study shows that as stated in hypothesis (H3), PassShapes entry is not as fast as entering PINs but remains within an acceptable range compared to them. Even more when considering the fact that for all the subjects drawing shapes with a stylus was an unfamiliar task as no one stated to use touch screen devices in everyday life. Entering PINs on the other hand was well-known and often executed by the subjects.

Regarding hypothesis (H4), we could show that even though the algorithm of the prototype can still be optimized, PassShapes did not perform significantly worse than PINs compared on their error rate. Thus, (H4) can be considered as confirmed.

Due to the reason that the differences in time are not drastic and the expected improvement accompanied with repeated usage, we consider these results regarding the usability promising. Moreover, this is confirmed by the fact that none of the participants complained about PassShapes, neither regarding the speed nor the error rate. More than 50% of them said they liked the concept and all mentioned that they are convinced that the technique works well.

Further prototypes implementing new algorithms incorporating findings from disciplines like character recognition may allow an even more robust stroke detection than the current prototype.

5. COMPARING PASSSHAPES TO OTHER GRAPHICAL AUTHENTICATION METHODS (RELATED WORK)

In this section the presented concept will be compared to other graphical authentication methods. Since the deficits of PIN and password-based authentication are known for years lots of research has been made to develop alternative authentication mechanisms. Special attention will be given to other graphical authentication approaches. According to De Angeli et al. [6], these can be classified into three groups: the locimetric, the cognometric and the drawmetric systems.

5.1 Locimetric systems

These systems require the identification and the selection of regions in an image. To specify a locimetric 'password' the user has to choose and select a sequence of regions on a picture by using a pointing device. In order to successfully authenticate to the system later, the same sequence of regions has to be selected by the user. This method is the oldest implementing graphical authentication and was patented in 1996 by Blonder [2]. A more up-to-date implementation is Wiedenbeck et al.'s *PassPoints* system [23]. These methods refer to the 'method of loci', a popular mnemonic where information is coded spatially by mentally associating it to well-known places, like places along an often traveled road.

Locimetric systems show good memorability but have some security and usability limitations: The security strongly depends on the used image. As the user has to choose several regions on the provided picture it must be assured that the used images contain enough regions that are of interest. Investigations made by Renaud et al. [19] show that most people tend to choose the same regions on standard pictures, which can make locimetric passwords predictable and thus easy to corrupt. Furthermore, the process of creating a password is quite complex as a picture has to be provided and the regions to be chosen. There is no possibility to create or reset a password by the system. Within the log-on process click accuracy is an issue and the log-on times are quite high (8.6 seconds).

5.2 Cognometric methods

This group of methods utilizes the superior capabilities of pictorial recognition memory. In order to create a

cognometric 'password' the users create a portfolio of several images selected from a large pool. On the log-on screen the users are presented a set of pictures, some taken from their portfolio, and some selected randomly. For successful authentication the users now have to select 'their' pictures amongst the distractors. An example for one of these methods is the Déjà-Vu system by Dhamija and Perrig [10]. A specialty of this system is the fact that so-called 'random-art' pictures are used. These pictures are generated by a random generator. So the system only has to store seed values for the generator, but no pictures itself.

This method also shows good memorability, but again there are some limitations regarding security and usability: With cognometric methods it is difficult to create 'passwords' that derive from a large password space. Complexities as for numeric PINs are no problem, but to achieve the same complexity as passwords composed of six characters it would be necessary to identify 16 pictures out of 40 during the authentication process without an error, which should be rather difficult and time-consuming. The cognometric systems have the same problems as the locimetric systems regarding convenience and usability. Again the password creation process is quite complex and passwords cannot be assigned by the system. The log-on times are high (32 seconds) which can affect user acceptance.

Another popular example for a cognometric method is the PassFaces system provided by the *Real User Corporation* [18]. Here the superior capabilities of humans in distinguishing faces are exploited. The user builds a portfolio containing faces. When authenticating the users have to select 'their' faces amongst a set of distractors. The PassFaces method provides a good memorability as investigations made by Brostoff and Sasse [3] can prove. But other studies dealing with the security of the system can identify problems. Davis et al. find that users prefer to choose faces of their own sex and race or attractive faces, what makes the choices predictable [5].

5.3 Drawmetric methods

The here presented PassShapes belong to the group of drawmetric methods. Drawmetric systems require the users to draw a preset figure in order to authenticate themselves. A well-known system is 'Draw-a-Secret' by Jermyn et al. which was presented in 1999 [13]. Using this system originally designed for authentication on PDAs the user defines a 'password' by drawing a picture on top of a grid. It is claimed to be more secure than traditional passwords due to its large password space. The complexity of six-character alphanumeric passwords is realized by drawings consisting of only eight strokes. The system uses the sequence of the coordinates of the grid cells used by the drawing for its internal representation. This means the representation of a password consists of coordinates in the form (0,0), (1,0), (2,0), (2,1), etc. Therefore no image data has to be processed and stored. For authentication the users have to reproduce their previously defined drawing starting from the exact same cell and ending in the exact same cell.

Due to the usage of the grid-cells the drawing accuracy does not have to be perfect. But there still remain some problems regarding accuracy: The drawing has to be started in the right grid-cell and touching the grid when drawing is critical since the algorithm may not be able to define which cell the users intended to hit. Using diagonals is also problematic as the adjacent cells could be hit accidentally. Investigations made by Nali and Thorpe reason, that 29% of the produced Draw-a-Secret drawings have to be classified as invalid [15]. Other research in this area done by van Oorschot and Thorpe tries to model the users' choice in creating drawings [16]. They identify that the theoretical size of the password space is not exploited. Users tend to create drawings that are highly symmetric and positioned in the center of the grid. These findings restrict the security of the system as the probability to guess the right 'password' grows and dictionary like attacks could successfully be used. Regarding this it must be stated that the number of password space is still quite large – the complexity of a six-character alphanumeric password is reached when ten-stroke drawings are used if the results of van Oorschot and Thorpe are taken into account.

Interestingly, no studies have been conducted that tested the memorability of the Draw-a-Secret system, although there have been analyses of the security of the system.

5.4 Comparing the PassShape system to other systems utilizing graphical authentication

The PassShapes presented in this work are functionally similar to the Draw-a-Secret (DAS) system. But we believe our approach overcomes some limitations of DAS. First, no grid is needed to draw a PassShape. So the users do not have to remember a specific starting point and do not have to take care of touching the grid while drawing. As the strokes that PassShapes can be composed of always differ in a minimum angle of 45° and only the edges are necessary for the detection of PassShapes drawing accuracy is not a big issue. Furthermore the length of the single strokes or the size of the PassShape does not matter. Creating PassShapes and authenticating using PassShapes can be considered more usable than the DAS scheme.

Another advantage is the fact that due to their simple structure, PassShapes can easily be created by a random generator. So 'passwords' can be reset by the system and automatically generated for new users. In distinction to the other presented graphical authentication systems no time-consuming processes are necessary to incorporate new users. Evaluating the security of the system, it is reasonable to assume that the findings made regarding symmetry in user choice will also apply to the PassShapes. But as for

the DAS system the password space will still be large enough to provide sufficient security. Compared to the locimetric and cognometric systems PassShapes can provide a higher security. As outlined before, the security of the locimetric methods like the PassPoints system strongly depends on the used images. The users tend to choose very similar regions on the used pictures. Dirik et al. even provide a model to predict the points of interest used for creating login sequences [9].

The cognometric approaches suffer from the small password space and systems using real pictures instead of the random art used in the presented Déjà-Vu system are facing the problem that attackers equipped with knowledge about their targets can guess the used secret pictures by taking into account the target's preferences. Analyses of the PassFaces system show that users prefer to choose faces of their own race and sex or attractive faces.

6. FUTURE WORK

From the first idea to the final realization and evaluation, the PassShape concept has been changed and adapted several times. As usual, during the work and mainly during the evaluations, several possible extensions and improvements were found as well as additional directions of investigation. In this section, the most interesting ideas are outlined.

In another project that focused on evaluating eye-gaze interaction as a private and secure input method for public terminals [7], the idea was born to use gestures performed with the eyes to authenticate users to an ATM. The approach utilized gestures to perform the numbers of a PIN with the eyes. Unfortunately, this resulted in a cognitive overload of the users since they had to remember the different gestures for the different numbers which was significantly slowing down the interaction speed as users had to recheck the gestures for certain numbers during execution. Therefore, the idea came up to combine this approach with PassShapes to provide a secure and easy to remember authentication method for public terminals. A new project dealing with this approach is already running and delivered first encouraging results [8]. Fortunately, the underlying stroke concept perfectly fits the movement of the eyes that can only move in saccades. Thus, PassShapes are suited to be executed as eye-gestures.

Additionally, it seems interesting to evaluate the users' choice regarding PassShapes. As mentioned earlier for other graphical passwords, a problem is that users tend to choose similar or easy to guess 'passwords' if they are allowed to create them by themselves. This decreases the size of the possible password space. Therefore, we are currently working on a web based version of PassShapes which will be used to investigate this kind of user behavior including the question "What kind of PassShapes will users choose?". It is also planned to offer PassShapes as an alternative authentication method for real online services (in parallel to the password authentication). So evaluations on user acceptance and behavior in situations of real use and real importance can be performed.

Another interesting aspect that has not been addressed yet is the behavior regarding multiple PassShapes. That is, will users be able to remember several different PassShapes for different purposes? Will they choose similar PassShapes for different purposes? Will they develop specialized mnemonic strategies to further increase PassShape memorability? A possible strategy could be that users define shapes using associations to the purpose of authentication, which could raise security threats due to knowledge based guessing attacks. For example users could choose a PassShape in the shape of a mobile phone as an authentication token for their mobile device.

Finally, it seems worthwhile to investigate the usability aspect of PassShapes in a longitudinal study design. Even though the first usability evaluation shows promising and satisfying results regarding interaction speed and error rate, we expect the speed of PassShapes to rise significantly over time. Therefore, it would be interesting to evaluate whether or not users will be able to perform PassShapes as fast or even faster than standard PIN entry with our system.

7. CONCLUSION

Summarized, the PassShapes system introduced in this paper shows encouraging results in the conducted studies. The simple stroke based drawings show a good memorability if the strategy of repeated drawing is used and the PassShapes are trained by reproducing them multiple times. As discussed in section three the advantages are caused by the pictorial superiority effect, the higher depth of processing and the involvement of motor memory.

The first results regarding usability are also promising. The log-on times using PassShapes are slower when compared to traditional PIN entry, but much faster when compared to other alternative approaches using graphical authentication. When taking into account that drawing on a touch screen is not very familiar to average users at the moment it is reasonable to assume that frequent usage will lead to a reduction of PassShape input times. In this context it can be mentioned that the metaphor of drawing a specific shape in order to authenticate is well-known and also widespread in our everyday lives: Each time we sign a check or a contract we prove our identity with our characteristic signature. But as mentioned above further user studies should be conducted in order to evaluate the usability of the PassShapes concept. Especially the memorability of multiple PassShapes and user satisfaction should be investigated thoroughly.

A big advantage of the PassShapes concept is the fact that simple character strings can be used for their internal

representation. So the entire security architecture of a current password or PIN-based system can be reused. PassShapes can be stored in the same databases, transmitted with the same protocols and secured with the same hash functions and ciphering methods as used for current authentication systems. Only the client systems have to be equipped with some hardware supporting the production of simple drawings and some software implementing a PassShape detection algorithm. In contrast to other systems utilizing graphical authentication neither the storage nor the transmission of image data is necessary. This also simplifies the introduction of the system. It is possible that some users still authenticate using traditional passwords or PINs whereas others already use PassShapes. The PassShape system is also system administrator friendly – PassShapes can be generated at random and they can be set and distributed by the system automatically.

8. REFERENCES

[1] Adams, A., Sasse, M. A. 1999. Users are not the enemy. In: *Communications of the ACM*, 42:12, 40-46.

[2] Blonder, G., 1996. Graphical passwords. United States Patent 5559961.

[3] Brostoff, S., Sasse, M.A. 2000. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In: *Proceedings of the HCI 2000*. 405-424.

[4] Craik, F. I. M., Lockhart, R. S. 1972. Levels of processing: A framework for memory research. In: *Journal of Verbal Learning and Verbal Behavior*, 11.

[5] Davis, D., Monrose, F., Reiter, M. K. 2004. On user choice in graphical password schemes. In: *Proceedings of the 13th USENIX Security Symposium*, (San Diego, California, August 9-13), 151-164.

[6] De Angeli, A., Coventry, L., Johnson, G., Renaud, K. 2005. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems, In: *International Journal of Human-Computer Studies*, 63:1-2, 128-152.

[7] De Luca, A., Weiss, R., Drewes, H. Evaluation of Eye-Gaze Interaction Methods for Security Enhanced PIN-Entry. In: Proceedings of OZCHI 2007, Adelaide, Australia, 28 – 30.11.2007.

[8] De Luca, A., Weiss, R., Hußmann, H., and An, X. 2008. Eyepass - eye-stroke authentication for public terminals. In CHI '08 Extended Abstracts. Florence, Italy, April 05 - 10, 2008.

[9] Dirik, A. E., Memon, N., Birget, J. 2007. Modeling user choice in the PassPoints graphical password scheme. In *Proceedings of the SOUPS 2007,* (Pittsburgh, Pennsylvania, July 18 - 20, 2007).

[10] Dhamija, R., Perrig, A. 2000. Déjà Vu: a user study using images for authentication. In: *Proceedings of the 9th Conference on USENIX Security Symposium* (Denver, Colorado, August 14 - 17, 2000), 45-58.

[11] Flores d'Arcais G. 1994. Order of strokes writing as a cue for retrieval in reading chinese characters. In: *Europ. Journal of Cognitive Psychology*, 6:4, 337–55.

[12] Klein, D. 1990. Foiling the cracker: A survey of, and improvements to, password security. In *Proceedings of the 2nd USENIX Security Workshop* (Portland, Oregon, August 27, 1990), 5-14.

[13] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., Rubin, A. D. 1999. The design and analysis of graphical passwords. In: *Proceedings of the 8th USENIX Security Symposium* (Washington, D.C., August 23–26,1999), 1-14.

[14] Naka, M., Naoi, H. 1995. The effect of repeated writing on memory. In: *Memory & Cognition*, 23:2.

[15] Nali, D., Thorpe, J. 2004. Analyzing User Choice in Graphical Passwords. Tech. Report TR-04-01, School of Computer Science, Carleton University, Canada.

[16] Oorschot, P. v., Thorpe, J. 2008. On predictive models and user-drawn graphical passwords. In: *ACM Transactions on Information and System Security (TISSEC)* 10:4, 1-33.

[17] Paivio, A., Csapo, K. 1973. Picture Superiority in Free Recall: Imagery or Dual Coding? In: *Cognitive Psychology* 5, 176-206.

[18] Real User Corporation. PassFaces Personal. http://www.passfaces.com.

[19] Renaud, K., De Angeli, A. 2004. My password is here! An investigation into visuo-spatial authentication mechanisms. In: *Interacting with Computers*, 16:6.

[20] Sasse, M.A., Brostoff, S., Weirich, D. 2001. Transforming the 'weakest link': a human–computer interaction approach to usable and effective security. In: *BT Technology Journal* 19:3, 122–131.

[21] Shadmer, R., Brashers-Krug, T. 1999. Functional Stages in the Formation of Human Long-Term Motor Memory. In: *The Journal of Neuroscience*, 17:1.

[22] Standing, L., Conezio, J., Haber, R.N. 1970. Perception and memory for pictures: Single-trial learning of 2500 visual stimuli. In: *Psychonomic Science* 19:2, 73-74.

[23] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., Memon, N. 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. In: *International Journal of Human-Computer Studies (HCI Research in Privacy and Security)* 63, 102–127.