Look into my Eyes! Can you guess my Password?

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

Martin Denzel
Media Informatics Group
University of Munich
Amalienstr. 17
80333 Munich, Germany
denzel@cip.ifi.lmu.de

Heinrich Hussmann
Media Informatics Group
University of Munich
Amalienstr. 17
80333 Munich, Germany
hussmann@ifi.lmu.de

ABSTRACT

Authentication systems for public terminals – and thus public spaces – have to be fast, easy and secure. Security is of utmost importance since the public setting allows manifold attacks from simple shoulder surfing to advanced manipulations of the terminals. In this work, we present *EyePassShapes*, an eye tracking authentication method that has been designed to meet these requirements. Instead of using standard eye tracking input methods that require precise and expensive eye trackers, EyePassShapes uses eye gestures. This input method works well with data about the relative eye movement, which is much easier to detect than the precise position of the user's gaze and works with cheaper hardware. Different evaluations on technical aspects, usability, security and memorability show that EyePassShapes can significantly increase security while being easy to use and fast at the same time.

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

Performance, Reliability, Security

Keywords

Eye gestures, EyePassShapes, eye tracking, authentication, privacy, security

1. INTRODUCTION

Improving authentication is a goal that researchers already try to achieve for a long time. Even though the number of services and systems we authenticate to has increased drastically over the past decades, the prevailing method is still the same: passwords or personal identification numbers (PINs) are used to authenticate a person to a system. Passwords as well as PINs have manifold well-known security and usability flaws. In public spaces – the spaces in which more and more authentication processes take place – one of these problems becomes most crucial, and this is the possibility to steal the secret information. Within the last years, attacks on public terminals, mostly cash machines (ATMs), have increased significantly. Miscellaneous attacks have been developed out of which shoulder surfing is still one of the most common and simplest attack [16]: an attacker tries to see the user's PIN from a close spot while it is entered at the ATM. Even though those attacks create a significant financial damage every year, increasing security does not obtain as much attention as it deserves. Some ATMs are equipped with modifications that try to hide the input from onlookers but these measures are easy to be outtricked, too.

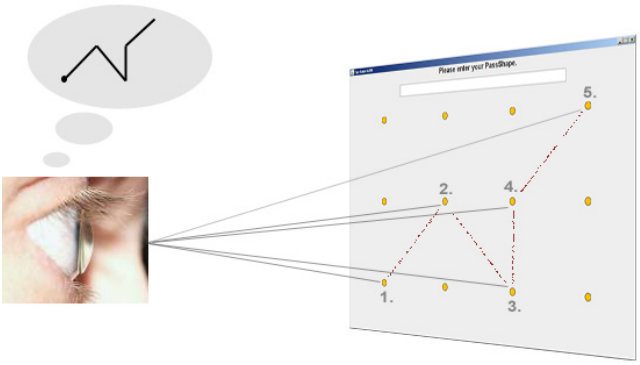


Figure 1: EyePassShapes: a user performing the gesture "93U9".

Increasing security by obvious measures like longer passwords does not solve the problem since special properties of authentication in public spaces have to be considered:

- Public authentication is time-critical. Users want to finish their tasks quickly, and there might be other people waiting for the same terminal. Any unacceptable overhead might lead to frustration.
- The authentication token should be easy to remember.
- Authentication has to be secured against a huge variety of attacks aiming to steal the secret information.

Symposium on Usable Privacy and Security (SOUPS) 2009, July 15–17, 2009, Mountain View, CA USA
.

- And finally, authentication methods have to be easily deployable since in case of a system change, a big amount of terminals would have to be changed accordingly.

It is often argued that biometric verification will solve these problems in the near future since it is fast, cannot be forgotten and – if the hardware becomes cheaper – can be easily deployed. Nevertheless, biometrics have their own specific problems. It is still very error prone. For instance, fingerprint scanners are very sensitive to changes in the humidity of the air. The main drawback however are privacy concerns. Biometric features are lasting and unchangeable. Once recorded or given away – for example to a supermarket – the owner has no more control over it. Such privacy concerns are even amplified by recent successes of German hackers to copy and publish the fingerprints of an important politician. Thus, it is still worthwhile to evaluate and improve anonymous *something you know* authentication systems.

Based on past experiences with authentication systems, in this paper we present *EyePassShapes*, an authentication system utilizing eye tracking technology. Authentication is achieved by performing simple gestures – creating shapes – with the eyes as shown in figure 1. The technological requirements for EyePassShapes are quite low which makes it more appropriate for public authentication than existing concepts based on eye tracking [12, 5]. For instance, low cost and low weight eye tracking systems that can record relative movement are sufficient. The system tries to overcome the weaknesses of other authentication systems [5, 23], keeping their advantages and omitting the problematic parts. Moreover, EyePassShapes was created taking into account the previously mentioned properties of public authentication systems.

While in [6] the idea of EyePassShapes has been briefly discussed as work in progress, in this paper we will go from theory to practice. We will present a thorough and extensive evaluation of all aspects of the system: design, usability, memorability and security.

2. RELATED WORK

2.1 Eye Gestures

Gaze based interaction techniques is a rather old field of HCI. Techniques like dwell time have already been evaluated in the late 80s and early 90s [11]. The concept of eye gestures on the other hand is quite new.

For a long time this approach has been neglected. Drewes et al. were the first to show that using eye gestures for specific input tasks actually can make sense and that users can intentionally create these shapes using their eyes [9]. Those results encouraged us to utilize eye gestures for the EyePIN system [5].

Currently, other researchers performed thorough analysis of interaction systems based on eye gestures. For instance Wobbrock et al. [26] evaluated text input based on eye gestures. Bulling et al. even created an eye tracking device which, due to its nature of recording relative movements rather than exact points, perfectly fits the eye gestures concept [1]. These results further encouraged us to follow the idea of using eye gestures for authentication purposes.

2.2 Authentication

Authentication systems are often categorized the following way: *something you have*, *something you know* and *something you are*. It is not unusual that systems fall into several of these categories. Another interesting way to look at authentication systems is to distinguish between systems that try to increase security and usability of traditional authentication methods like PIN and password and systems that break completely new ground. Talking about authentication in public spaces, we argue that a third categorization is more appropriate since it better reflects the advantages and disadvantages of the different techniques with respect to the characteristics and requirements of authentication in public spaces: purely *software based*, *hardware based* and *user hardware based* approaches. Needless to say, combinations of those categories are possible as well.

2.2.1 Software Based Authentication

Software based authentication systems represent the simplest approach. They rely on available output and input hardware of public terminals. Therefore, in most cases, simple software updates do the trick. Considering the huge amount of public terminals this is a noticeable financial advantage for the service provider. Unfortunately, most of those systems add a significant overhead to the input and provide shoulder surfing resistance only but are not resilient against video attacks and the like.

Cognometric passwords, that is passwords that require the users to find a specific picture within a set of distracting pictures, provide authentication tokens that are easier to remember. The approaches are manifold: some use random art pictures like in [8] while others use photos of persons like VIP [3] by De Angeli et al. VIP has also been intensively tested on usability and feasibility for use at ATMs [3, 14]. However, cognometric systems do not increase security but only usability. Thus, current research focuses more and more on the security aspect as well. For instance, Use Your Illusion by Hayashi et al. [10] utilizes obfuscation techniques to add enhanced security to graphical password schemes.

Other software based authentication systems focus more on security. The convex hull click scheme by Wiedenbeck et al. [24] randomly displays a big set of small icons on the screen. At least three of them are part of the user's set of icons. To authenticate, the user has to mentally form an area which is delimited by her icons and click one of the other icons within that area. Thus, no information about the user's icons are given away to an observer. The best way to attack this system is by repeated filming. Differences can reveal the user's icons. Increasing security of PIN-entry at software level has been the goal of the system created by Roth et al. [17]. It hides the real PIN with a four step trapdoor game based on color encoding of the numbers. This means, for each number of the PIN the user has to press four times, which creates significant overhead to the PIN-entry. Additionally, the system is not resilient against camera attacks. Finally, Tan et al. [21] created the spy-resistant keyboard, which can hide arbitrary input from onlookers (does not prevent camera attacks) by adding overhead to the input, which is impossible to follow without proper recording.

2.2.2 Hardware Based Authentication

A more costly way to enhance security of public authentication is to add additional hardware to public terminals.

Besides the costs, the main weakness of these approaches is that the devices are publicly available 24 hours a day, seven days a week in the worst case and thus it becomes easy for attackers to manipulate them.

In many cases the additional hardware is used to provide an invisible communication channel to the user and transfer secret information, which is used to secure the authentication. For instance, Undercover by Sasamoto et al. [18] uses tactile feedback created by the movement of a rotating ball to communicate a keyboard layout to the users that they have to use to authenticate. Another system that uses tactile feedback to affect the user's input is presented by Deyle at al. in their work on authentication via tactile PIN-entry [7].

Other research uses additional hardware for input rather than for output. One of the most famous approaches is a typical *something you are* technology – biometry – as evaluated by Coventry et al. for the use at ATMs [2]. Malek at al. [13] use a combination of pressure sensors with graphical password to enable spy-resistant authentication. Thorpe et al. [22] theoretically describe a system that could read the password from the user's mind considering ethical hurdles more than technological ones. Finally, Kumar et al. evaluated common eye-tracking interaction techniques on their appropriateness for authentication [12]. Their results are like what we found in [5].

2.2.3 User-Hardware Based Authentication

Finally, systems based on hardware owned directly by the user have the potential to eliminate the two main weaknesses of the hardware based approaches. Firstly, it does not create additional costs for the service/terminal provider since hardware is employed that is already owned by the user. Since this hardware is not available to an attacker, it cannot be manipulated as is the case for hardware connected to a terminal. While user hardware overcomes those weaknesses, it opens new ways for attacks. For instance those systems often rely on wireless communication with the terminal which makes them vulnerable to man-in-the-middle attacks.

A system that utilizes motion sensors of modern mobile devices is presented by Patel et al. [15]. In order to authenticate with a terminal, the user has to shake the mobile device in a predefined way. We created a prototype called VibraPass [4], which uses the mobile device of the users as an additional output channel. Tactile feedback is used to add an overhead of lies to PIN-entry to hide the real PIN from attackers. The knowledge about which part of the PIN is true and which is a lie is shared between the terminal and the user via this tactile feedback.

2.2.4 Talking about EyePassShapes

Regarding the previously mentioned categorizations, EyePassShapes is a *something you know* authentication system based on *additional hardware* (eye-tracker) that does not try to increase security of standard authentication approaches like PIN or password but is built upon an *alternative authentication mechanism*, PassShapes [23]. Combining different concepts, it tries to overcome their weaknesses. It is easier and cheaper to deploy than standard eye tracking systems since it does not require to know the exact position of the user's gaze and thus no calibration, which also makes it extremely robust and appropriate for outdoor situations. It is also more secure than PassShapes due to the use of eye-tracking technology, which hides the input from attackers.

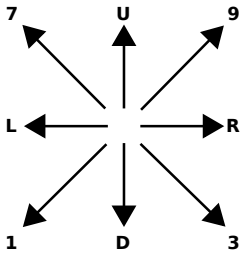


Figure 2: PassShapes can consist of arbitrary combinations of eight different strokes. The characters are used for the internal representation of a shape.

3. CONCEPT

As mentioned, EyePassShapes extends and improves two authentication methods by combining them. This way, their flaws are eliminated and replaced with the advantage of the respective other. The two systems that have been extended are PassShapes [23] and an authentication system based on eye gestures which we will refer to as EyePIN [5] for the sake of ease.

3.1 PassShapes

We created PassShapes as an alternative authentication approach for improved memorability. To authenticate with a system, the users have to paint shapes – consisting of strokes – in a predefined order. There are eight possible strokes as depicted in figure 2. A PassShape consists of an arbitrary amount of those strokes. Internally, PassShapes are represented as a string, which makes them appropriate for standard security mechanisms like hashing. For instance, the internal representation for the PassShape for up, right, down, left (a square) would be *"URDL"*.

Theoretically, increased memorability is achieved in two ways: Firstly, the authentication tokens are based on shapes which are essentially pictures. Thus, the *pictorial superiority effect* [20] – simply speaking, pictures can be more easily remembered than abstract tokens like numbers – should increase memorability. Second, PassShapes are always drawn in the same way following a specific order. Thus, *motor memory* effects [19] can positively influence their memorability. A longterm user study could reveal advantages of PassShapes if repeated writing strategies are used.

The main disadvantage of PassShapes is that it does not increase security compared to PIN or password entry. Whenever a user draws her PassShape, nearby onlookers can easily steal it. Thus, most of the attacks that work on PINs and passwords can be used for PassShapes as well.

For more information about PassShapes refer to [23].

3.2 EyePIN

When creating the concept for EyePIN, we set a focus on security rather than on usability. The authentication token remains the user's standard PIN. Security is increased by changing the input method. Instead of typing the number, the user performs eye gestures that represent the respective digits. The gesture alphabet for EyePIN (see figure 3) is based on EdgeWrite by Wobbrock et al. [25]. Since EyePIN requires digits only, it utilizes a simplified version of EdgeWrite. Due to the fact that gestures can occur unwillingly in normal gaze the user has to press a control key,

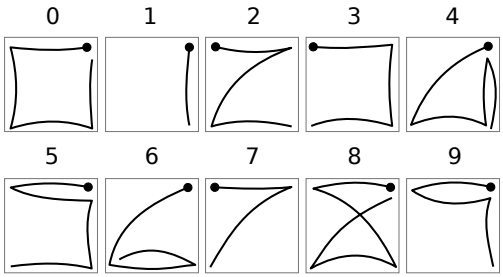


Figure 3: The gesture alphabet used for EyePIN.

which indicates to the system that a gesture will be performed and should be analyzed.

In [5], we compared EyePIN to PIN-entry based on standard eye tracking interaction methods. The results indicated that EyePIN is more appropriate for public authentication. On the one hand it is more robust to input errors and on the other hand – which is more important – it is easier and cheaper to deploy. This advantage is based on an important characteristic of EyePIN: it does not require the exact position of the user's gaze on the screen. Recognition of relative movements is already adequate. Thus, low cost and low weight eye trackers meet its requirements. Another advantage is that it does not require calibration.

The evaluation of EyePIN revealed some serious disadvantages. For instance, interaction times were poor compared to other techniques. A bigger problem was the high memory load created by the new alphabet of gestures that had to be understood and used. The users did not only have to remember the digits of their PIN but also the way to input each of those digits, which created a big overhead due to attention shifts between the terminal and the alphabet list which had been printed for them.

3.3 Combining the Two – EyePassShapes

EyePassShapes – first time theoretically discussed in [6] – uses the stroke based authentication tokens of PassShapes and combines it with the secure eye tracking approach of EyePIN. Fortunately, the strokes used for PassShapes perfectly fit the biological constraints of the human eye, which moves in saccades and cannot perform any non-linear movements. Thus, PassShapes did not have to be adapted in any way to be appropriate for eye gesture input.

Just like PassShapes, EyePassShapes can be performed in one time but also in as a row of consequent shapes (release the control key and press again).

Authentication with EyePassShapes works as follows (see figure 1 for an example):

1. To enter the PassShape, the user holds down the control key.
2. Whenever the button is released, the movements that have been done by the user's eye are analyzed.
3. After entering the whole PassShape, the user ends the authentication by pressing an "ok"- button.
4. Finally, the shape (or the combination of all if the user pressed several times) is compared to the PassShape in the database. If they match, the authentication approach was successful.

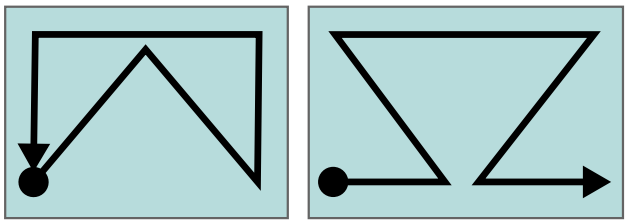


Figure 4: Two examples of PassShapes for the EyePassShapes system. Left: "93ULD". Right: "R7R1R".

By relying on easy-to-use authentication tokens which are highly appropriate for eye gaze input (PassShapes), EyePassShapes should be easier to use than EyePIN. At the same time, it should be more memorable than standard PIN and password (and thus also EyePIN). An interesting question is whether motoric memory effects can be observed when PassShapes are entered with the eyes. At the same time, using an eye tracking input method makes it more secure than standard PassShapes due to its shoulder surfing resistance. Figure 4 shows examples of two PassShapes that could be used in the EyePassShapes system. Both consist out of five strokes.

4. PROTOTYPE

The prototype of EyePassShapes – as depicted in figure 5 – consists of the commercial eye tracker ERICA[1] and a Windows tablet PC. The EyePassShapes software has been written in C++ (proxy to the eye tracker) and JavaSE (gesture recognition and user interface). The space button has been chosen to represent the control key necessary to control the gesture recognition. To find the right settings for the EyePassShapes software, a user study has been conducted.

4.1 Technical Evaluation

Creating the prototype software started with one main question: *Should visible aides be provided and if yes, of which kind?*

This question refers to the choice of a background image. Should the background provide points or other visual markers that the user can fixate on (visual aides)? In [9], Drewes et al. let the users perform very simple gestures like squares and tested different backgrounds. They chose a blank, a spreadsheet (simulating a work environment) and a grid background consisting of lines. They could show that with all designs (even with the blank screen) users performed rather well. But a deeper look at the data revealed that even for the blank screen the users created themselves visual aides. For instance they used the screen corners or dirt stains on the screen to help them control their gaze. These tricks worked fine for the simple gestures used in [9].

Since the PassShapes used for EyePassShapes are slightly more complex than the gestures tested by Drewes et al., a more advanced evaluation of the backgrounds for the final prototype seemed appropriate. Informal evaluations showed that only advanced EyePassShapes users could perform the shapes on a blank screen. Other screen designs could be neglected as well. In the end, two possible designs remained as

[1]http://www.eyeresponse.com, February 2009.

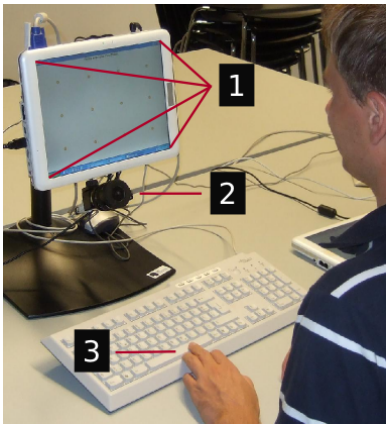


Figure 5: EyePassShapes prototype: 1. Field of vision. 2. Eye tracker. 3. Control key.

depicted in figure 6. One consisting of simple points while the other is similar to the grid design used in [9]. Both designs allow the user to input shapes with a horizontal span of three and a vertical span of two strokes. That is, EyePassShapes that fit in this area can be performed as a single stroke. If a shape requires more horizontal or vertical space, it has to be performed in several steps.

With respect to the eye tracker available, another rather simple question was on the appropriate grid size. Since the ERICA eye tracker is position based, it was important to choose an appropriate pixel value (a grid size) that denotes whether a stroke has been performed or not. Also with respect to the screen size and resolution of the eye tracker this value has to be chosen carefully. For eye trackers that only record relative movement, like the system designed by Bulling et al. [1], this step can be omitted. Informal evaluations and analyses favored 100 pixel and 150 pixel.

To find the best settings and the optimal design, we performed a formal user study.

4.1.1 User Study Design

The technical evaluation was performed using a repeated measures within participants factorial design. The independent variables were *background image* (dots and grid as shown in figure 6) and *grid size* (100 and 150 pixel). Thus, four different configurations have been validated against each other: dots + 100px, dots + 150px, grid + 100px and grid + 150px. The background picture had been optimized for the respective pixel size. To minimize the influence of the PassShape on the results, each participant performed each of the configurations with two randomly generated PassShapes. Each PassShape fit the constraints of the background picture and could theoretically be performed in one attempt. The order of the configurations was randomized to minimize learning effects. The dependent variables measured were speed, error rate and user satisfaction.

4.1.2 Procedure

For each participant, the evaluation started with a thorough explanation of EyePassShapes and the tasks that had to be performed. Then, a randomly selected configuration was assigned to the participant. An initial training phase allowed the user to get accustomed to the interaction. When

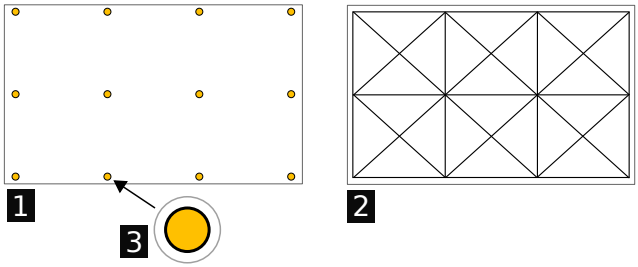


Figure 6: The two background designs for the EyePassShapes prototype: 1. Dotted background. 2. Grid. 3. Magnification of a dot.

she felt ready, the tasks started. With each configuration, the participant had three tries to successfully authenticate. Correct authentication or three times failure ended the current task. In the end, a questionnaire was used to collect basic demographic data and user experiences.

4.1.3 Participants

For the technical evaluation, ten volunteers had been recruited. This number seemed appropriate since the goal of the study was not an extensive evaluation of the system but to find the right settings for the prototype. The average age was 33 years. The oldest participant was 60, the youngest 23. Only one of them had ever used an eye tracker before.

4.1.4 Results

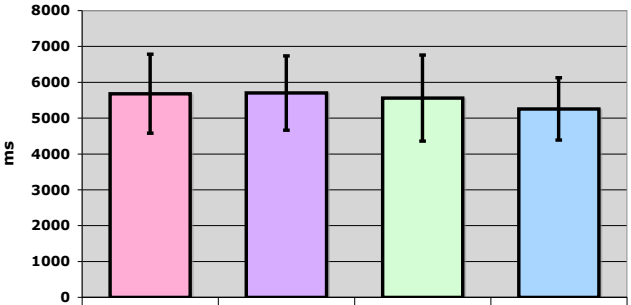
Having ten participants, each performing four tasks with two different PassShapes, results are based on 10x4x2=80 data sets. All PassShapes had been performed as one stroke. That is, no participant performed the shape in several consequent steps, which would be possible and was an option during the study.

Table 1: Numbers of authentication attempts that failed during technical evaluation.

grid 100px	grid 150px	dots 100px	dots 150px
4/17	3/17	0/17	2/17

An important aspect of the technical evaluation was how many authentication attempts could be completed successfully. Table 1 shows the numbers of failed authentication attempts for each configuration. Failed means the PassShape could not be entered successfully three times in a row. An explorative analysis of the data identified three different outliers in the data sets. Therefore, for each configuration, 17 valid inputs remained. As table 1 outlines, only the configuration with the dotted background with 100 pixel grid size did not lead to any failed authentication attempt. The numbers indicate that the dotted background seems to have a positive influence on error rate while the grid size does not affect it. However, a 2 x 2 (*background image* x *grid size*) within participants analysis of variance showed no significant main effects and no interaction effects (all $p>.05$).

Another indicator for an appropriate configuration are the interaction times needed by the participants to authenticate. Therefore, the times have been logged and analyzed. Only valid authentication attempts were considered in this evaluation. Eleven data rows fulfilled these criteria. Time was



	grid 100px	grid 150px	dots 100px	dots 150px
Mean	5678	5697	5556	5254
SD	2208	2076	2399	1741

Figure 7: Input times in milliseconds for the different configurations of the technical evaluation.

measured from pressing the space button (the control key) to releasing it. Figure 7 depicts the results of the analysis. Dotted with 150 pixel (M=5.3s, SD=1.7s) shows the best result. Grid with 150 pixel performed worst (M=5.7s, SD=2.1s). As for the error rate, a repeated measures within participants analysis of variance did not show any significant main or interaction effects (all $p>.05$).

Even though none of the results showed significance, there was a subjective tendency to prefer the dotted background. Furthermore, the analysis of the questionnaire showed that slightly more participants preferred using the dotted background to using the grid (six out of ten votes). These factors motivated our decision to use the dotted 150px configuration for further work (mainly evaluation) of the EyePassShapes prototype.

5. USABILITY EVALUATION

The final prototype has been used for a thorough usability evaluation of EyePassShapes. The study has been performed with the setup shown in figure 8. The whole process has been recorded with two cameras. The first camera was positioned directly opposite to the participant, filming the face. The second camera filmed the keyboard respectively the touchpad. To monitor and control the study, an additional screen and keyboard had been set up as well. The captured material served not only for usability but also for the security analysis.

In order to evaluate its usability, EyePassShapes has been compared to three authentication systems: standard PIN-entry, PassShapes using a touchpad and EyePIN. All systems have been installed on the user study PCs, EyePIN and EyePassShapes on the eye tracker, PIN and PassShapes on the tablet PC.

5.1 User Study Design

For the usability study, a repeated measures within participants factorial design has been chosen. The independent variable was *authentication method* with the levels PIN, PassShapes, EyePIN and EyePassShapes. That is, four authentication systems have been compared to each other. Standard PIN-entry represented the control condition, the baseline to judge the performance of the other systems. The dependent variables measured were error rate, speed and user satisfaction.

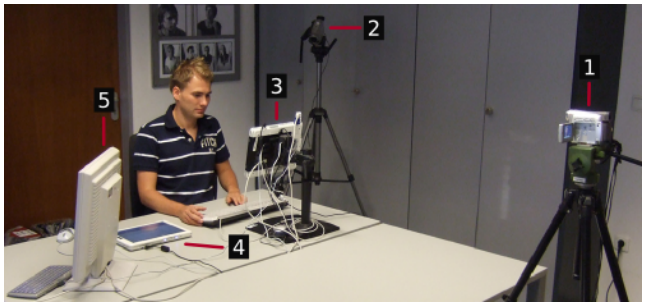


Figure 8: User study setting: 1. Front camera. 2. Back camera. 3. Eye tracker. 4. Tablet PC for PassShapes and PIN. 5. Surveillance monitor.

5.2 Procedure

In the beginning, the different systems and tasks were explained in detail to each participant. After drawing an ID from a bowl, the questionnaire was handed out to the participant. The first two pages had to be filled out immediately, while the rest of the questionnaire contained questions about the different prototypes. Thus, those parts had to be answered after the respective systems had been tested. The first two pages collected demographic data as well as information about the participant's experiences with eye tracking and touchpad systems. Additionally, data about the basic handling of PINs were asked. For instance, one question was in which situations the participants use authentication in public spaces and how they rate the importance of security, ease-of-use and speed of authentication systems.

For each prototype, the participant was provided with a thorough introduction followed by a trial phase that ran until the user felt familiar with the system. In this training phase, the participant could either choose an own authentication token or use one of the provided tokens. When the participant felt ready, she had to draw a random PIN or PassShape from another bowl. For each system, a new authentication token was drawn to minimize learning effects based on familiarity with the PIN/PassShape. The participant had three tries to authenticate with each token. After a successful authentication attempt or if failed for three times, the next part of the questionnaire was handed out to the participant before changing to the next system. This part of the questionnaire contained questions about ease-of-use, speed and security of the respective system. In the end, the last part of the questionnaire was given to the participant asking her to rate the systems with respect to each other.

For EyePassShapes, the participant could decide herself whether to perform the PassShape in one time or whether to individually perform different parts of the shapes by repeated pressing of the control button.

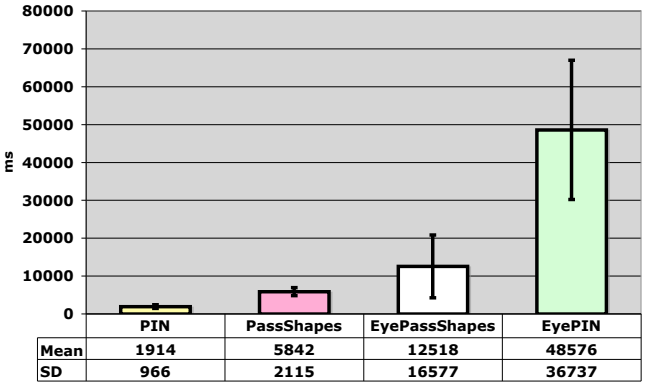
5.3 Hypotheses

Based on the experiences with the different authentication systems, the following hypotheses have been stated:

(H1) EyePassShapes is easier to use than EyePIN.

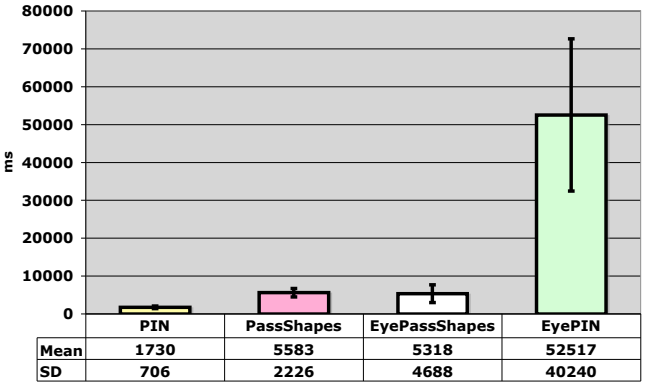
(H2) EyePassShapes is faster than EyePIN.

(H3) EyePassShapes is slower than standard PIN-entry.



	PIN	PassShapes	EyePassShapes	EyePIN
Mean	1914	5842	12518	48576
SD	966	2115	16577	36737

Figure 9: Input times in milliseconds for the different methods (all data).



	PIN	PassShapes	EyePassShapes	EyePIN
Mean	1730	5583	5318	52517
SD	706	2226	4688	40240

Figure 10: Input times in milliseconds for the different methods (data of the users that performed EyePassShapes in one stroke).

5.4 Participants

24 volunteers with an average age of 28 years participated in the user study. The youngest one was 22 and the oldest one was 40. 16 of them were male, eight were female. The majority of them – 19 out of 24 – never had used an eye tracking system before whereas only 8.3% stated that they never had used a touchpad before. Having 24 participants allowed perfect counterbalancing of the four authentication systems to minimize learning effects.

5.5 Results

5.5.1 Interaction Speed

To measure the time needed to authenticate using the different systems, the prototype created detailed log files in the background. Each event of any kind (key presses, strokes etc.) was logged together with a timestamp. For this evaluation, we decided to compare the times necessary for the pure authentication. That is, no additional times like the one needed for pressing the "ok" button in the end were added to the times. Therefore, the times were measured the following way:

Standard PIN: From pressing the first number to pressing the last number.

PassShapes: From first contact of the pen with the touchpad till the pen had been lifted the last time.

EyePIN/EyePassShapes: From pressing the control key for the first time to releasing it the last time.

Figure 9 outlines the results for the different methods. As expected, standard PIN-entry was the fastest (M=1.9s, SD=1.0s) and EyePIN was by far the slowest input method (M=48.6s, SD=36.7s). Surprising was the rather bad result for EyePassShapes (M=12.5s, SD=16.6s) which we expected to perform similar to PassShapes (M=5.8s, SD=2.1s). This was even more surprising because EyePassShapes performed noticeably better during the technical evaluation.

A one-way repeated measures analysis of variance showed that the authentication method had a highly significant influence on the input speed ($F_{1.34,28.17}$=25.14, p<.001). A post hoc analysis revealed that standard PIN was in a highly significant way faster than PassShapes and EyePIN (both p<.001) and was significantly faster than EyePassShapes (p<.05). This result supports hypothesis (H3). The advantage of EyePassShapes compared to EyePIN was also significant (p<.05), which supports hypothesis (H2). All other differences between the input methods were highly significant (all p<.001) with one exception: no significant result could be found between EyePassShapes and PassShapes (p>.4).

The surprisingly high input times for EyePassShapes combined with the non-significant result of the comparison between PassShapes and EyePassShapes led us to conduct a deeper analysis of the data for further clarification. It became quickly apparent that the difference in input times between PassShapes and EyePassShapes were due to a group of six participants that did not perform the EyePassShapes authentication in one stroke but in several consecutive strokes. That is, in contrast to the technical evaluation, some participants of the usability study decided to use the accumulative input technique for EyePassShapes.

Therefore, we performed an additional analysis splitting the results in two groups: one for those participants who had performed EyePassShapes in one stroke and one for those who used the accumulative method. The results showed that EyePassShapes was way faster when performed in one stroke (M=5.3s, SD=4.7s) than using the accumulative method (M=31.7s, SD=21.9s). When this insight was taken into account – i.e. considering only the data of the participants that performed EyePassShapes in one stroke – the results show a different picture as outlined in figure 10. A one-way repeated measures analysis of variance on the data set showed similar results to the analysis on the whole data set. The authentication method highly significantly affected the input speed ($F_{1.03,15.43}$ = 18.85, p = .001). Standard PIN-entry was significantly faster than the other methods (all p<.05, some p<.01). The result that EyePassShapes was faster than EyePIN was significant (p<.05). Those results give further support for (H2) and (H3). The small difference between PassShapes and EyePassShapes was not significant.

The results mostly match the subjective opinion of the participants. In the questionnaire, they were asked to rank the authentication methods regarding their speed. In average, standard PIN ranked first (M=1.04), PassShapes second (M=1.96), EyePassShapes (M=3.0) third and EyePIN (M=3.5) fourth.

Figure 11: Video material for the security analysis. Left: Front camera filming the user's face. Right: Back camera filming the user's hands.

5.5.2 *Ease-of-Use*

The interaction speed of the authentication methods gave first indications on their ease-of-use. To take a deeper look on that property, we relied on the subjective opinion of the participants. Firstly, the questionnaire contained questions in which the users were supposed to rate the ease-of-use of the different methods on a Likert scale from 1 (very difficult) to 5 (very easy). Additionally, the users were asked to rank the easiness of the different systems with respect to each other (ranks from 1 to 4). Another question that could give hints on the ease-of-use was on the experienced stress when using the different methods.

The evaluation of the questionnaire showed that standard PIN was rated the easiest (M=4.96), followed by PassShapes on the touchpad (M=4.13). EyePassShapes (M=2.67) and EyePIN (M=2.25) were rated averagely difficult. The fact that 19 of the participants had never used an eye tracker before but most of them were familiar with touchpads may have influenced that result.

Regarding ease-of-use, PIN was ranked first (M=1.13) and PassShapes was second (M=1.88). EyePassShapes (M=3.25) and EyePIN (M=3.29) ranked almost the same. The same amount of participants ranked EyePassShapes better then EyePIN and vice versa. This is a little bit surprising since the results of the interaction speed analysis showed that EyePassShapes was significantly faster than EyePIN. The results of the question regarding experienced stress were highly consistent with those results. Thus, hypothesis (H1) can only be accepted under reserve.

5.5.3 *Error Rate*

The error rate of an authentication system gives good hints about its practical value. Since normally authentication attempts in public spaces are limited to three tries – otherwise the bank card, credit card or access right might become blocked permanently – the error rate is crucial. In this evaluation we considered critical errors only. That is, a participant could not correctly authenticate with the system within three tries.

To our surprise, overall only two critical errors occurred, both with EyePassShapes. From past evaluations [5] it was shown that EyePIN is very resistant to errors since either a gesture for a number is either recognized or not and it is very unlikely to perform a wrong number. Even though the results of the comparison between EyePassShapes and EyePIN are not significant, it can be argued, that EyePIN has an advantage regarding the error rate.

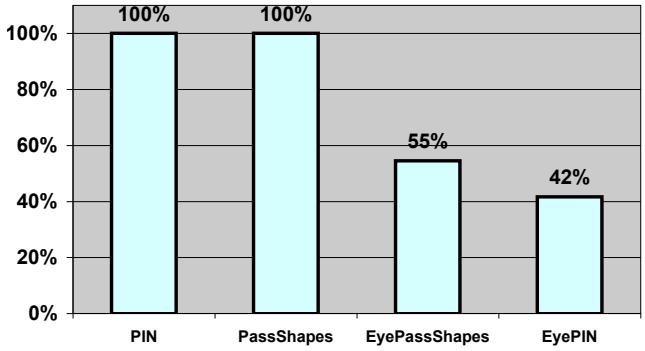


Figure 12: Percentage of successful attacks on the authentication methods.

6. SECURITY EVALUATION

The security evaluation of EyePassShapes was based on the data recorded during the usability study. In this analysis, the term *security* refers to whether the authentication tokens (PINs and PassShapes) of the different systems can be stolen via visual attacks like shoulder surfing or video recording. It should be found out whether the recorded information is sufficient for an attacker to extract the correct PIN or the PassShape. It should be noted here that EyePassShapes is fully resistant against shoulder surfing attacks. That is, an attacker cannot steal the password by simply standing close to the person using the system. In this analysis we evaluated highly advanced attacks based on video recordings.

As mentioned before, each participant had been filmed from the front and the side while using the authentication systems. Figure 8 shows the position of the cameras, the respective perspectives are depicted in figure 11. For each authentication method, 24 attempts were recorded this way. For the analysis, only successful authentication attempts were considered. Thus, for EyePassShapes, only 22 attempts were used for the security analysis.

In preparation for the security analysis, the video material was cut and ordered. To simulate the most effective attack on the systems, the final videos started when the authentication started and ended the moment the last number or stroke had been input. Most effective means that the attacker does not only have the recorded material but also the information about the exact timing (when the control key is pressed the first time and released the last time). This is important since gestures also occur in normal gaze [9] and thus knowing the point in time when the authentication started is a serious advantage for the attack. Any additional information within the videos that could reveal the PIN or PassShape had been made unrecognizable. For instance in figure 8 (right) the random PassShape of the user was visible on a paper and has been hidden with a hand symbol.

6.1 Procedure

The analysis of the video material – or better said the attack – was conducted by a person that had not been present during the user study. That person also had not participated in the creation of random PINs and PassShapes for the study. Thus, no helpful background information was available to that person. However, that person is an expert on EyePassShapes, PassShapes and EyePIN and thus had

Table 2: Detailed overview of the successful attacks on the different authentication systems.

	PIN	PassShapes	EyePassShapes	EyePIN
1. Try	23/24 = 95.8%	23/24 = 95.8%	07/22 = 31.8%	07/24 = 29.2%
2. Try	01/24 = 4.2%	01/24 = 4.2%	03/22 = 13.6%	02/24 = 8.3%
3. Try	–	–	02/22 = 9.%	01/24 = 4.2%
Overall	24/24 = 100%	24/24 = 100%	12/22 = 54.5%	10/24 = 41.7%

the best qualification for an attacker.

To analyze the video material, the attacker could use any video player and watch the clips as often as required. They could be stopped, rewinded, paused, analyzed frame by frame etcetera. Additionally, the attacker made notes on a provided list.

During the analysis, a second person (the observer) was present who had a list with the correct PINs and PassShapes. Whenever the attacker wanted to guess the correct answer, the observer gave a single "correct" or "wrong" statement. When the attacker guessed wrongly three times – which is the standard amount of trials for ATMs – the PIN or PassShape was marked as not recognized.

6.2 Hypotheses

The hypotheses of the security evaluation were:

(H4) EyePassShapes is more secure than standard PIN-entry.

(H5) EyePassShapes is more secure than PassShapes.

6.3 Results

Figure 12 shows the basic results of the security evaluation. Not surprisingly, due to the near to perfect observation of the input, all PINs of the standard PIN-entry and all PassShapes of the standard PassShapes system could be identified based on the analysis of the video material. The rates for EyePassShapes (55%) and EyePIN (42%) are around half that rate.

Taking a closer look at the results (see table 2) reveals an interesting trend. While almost all PassShapes and PINs could be identified in the first try, for EyePassShapes and EyePIN partially the second or third try was necessary for a successful attack. This can be explained by the fact that often strokes appear similar to each other. For instance it happened often that a stroke up ("U") was mistaken for a stroke up to the left ("7"), which then could be corrected in the second or third try.

A one-way repeated measures analysis of variance showed that the security of the authentication process was highly significantly affected by the system used ($F_{3,63} = 18.56$, $p<.001$). Post hoc tests revealed that the difference in successful attacks of EyePassShapes compared to standard PIN and PassShapes was significant (both $p<.05$). These results support hypotheses (H4) and (H5). The difference between EyePIN and PIN respectively PassShapes was highly significant (both $p<.001$). No significance could be found for the differences between EyePIN and EyePassShapes.

These positive results for EyePIN and EyePassShapes are supported by the questionnaire of the user study in which the users were asked to rank the different authentication system with respect to their security. For each system a rank from 1 (first, best) to 4 (last, worst) should be given. In average, EyePassShapes ranked best (M=1.75) closely followed by EyePIN (1.96). PassShapes ranked third (M=2.67) and standard PIN was ranked on four (M=2.92), thus considered the least secure system.

Additionally, we conducted an analysis whether the choice of the input strategy for EyePassShapes had an influence on the recognition rate. As mentioned before, EyePassShapes enables the users to input their PassShapes as one stroke or in several consecutive strokes (for example pressing the control key to perform the first part, release it and press again to perform the second part). Out of the 22 successful authentication attempts using EyePassShapes, 16 chose the one time strategy and six the accumulative method. Only one out of the six (17%) attempts using the accumulative method could be identified while eleven out of 16 (69%) attempts performing the PassShape in one attempt were found. It has to be noted here that this result is boosted by the fact that the attacker knew exactly when the gestures started and when they stopped.

Due to the small group of participants using the accumulative method, this large-looking difference is not significant ($p>.05$). However, it supports the assumption that PassShapes performed in one gesture are easier to find out. More generally, one can say that the main challenge of successfully stealing a PassShape lies in separating willingly performed eye movements from naturally occurring ones.

7. MEMORABILITY EVALUATION

For PassShapes, i.e. authentication by drawing pictures, a memorability study was carried out earlier, the results of which are published already [23]. There, memorability of PassShapes was evaluated in comparison to PINs. The evaluation showed that PassShapes could be more easily – and longer – remembered when the repeated input strategy was applied. That is, the PassShape is practiced several times within one session by actively drawing it. In this section, we report on a memorability study which investigated whether this effect can also be observed for the gaze gesture method EyePassShapes (i.e. when the PassShapes are performed with the eyes rather than drawn).

7.1 User Study Design

Since the evaluation should take place over several weeks and no participant should do more than one authentication method, a repeated measures inter-subject longitudinal experimental design was chosen. Three independent groups were formed to compare PassShapes, EyePassShapes and EyePassShapes with the repeated input strategy. That is, for group three, the memorability strategy was already pre-assigned. The independent variable was therefore *input strategy*.

To establish the same basic conditions as for the evaluation of PassShapes [23] – which would later on allow to estimate the performance in comparison to standard PIN-

entry as well – the randomly generated PassShapes used in the new study had the same number of strokes (seven) as in the previous study.

7.2 Procedure

The participants were randomly assigned to the three different groups. The assignment of a user to a group was decided by letting each participant draw a unique ID from a bowl. After that, each participant got a randomly generated PassShape. The PassShape was generated with the constraint of having a maximal horizontal extent of three and a maximal vertical of two. Therefore, each PassShape could – but did not have to – be performed in one stroke.

The participants were asked to take part in three different trials over the next weeks. The concrete tasks differed, depending on the group type. In the first and starting trial, the procedure was as follows:

Group 1 - PassShapes touchpad: After the random PassShape was assigned to a participant of group one, she was asked to try to remember it to reproduce it later on. For this, the participant had as much time as required and could use any strategy (none was explicitly mentioned by the observer). When the participant felt she could remember the PassShape, she signalized this to the observer. Thereafter, the paper with the PassShape was taken from her and she was asked to fill out a questionnaire collecting basic demographic data. Besides collecting the data, this part of the questionnaire was supposed to create a closure effect and make the participant believe the trial was over. When the questionnaire was filled out, the participant was asked to draw the PassShape. If the PassShape was wrong, it was shown again to the participant to remember it. In the end, a further questionnaire was handed out collecting information about the individual use of passwords and PINs.

Group 2 - EyePassShapes: The approach chosen for group two was analog to group one. The only difference was that participants in this group did not draw the PassShapes but performed them using eye gestures as required for EyePassShapes.

Group 3 - EyePassShapes repeated input: Finally, the approach for group three was the same as for group two with the difference that the learning strategy was assigned to the participants. After they got their PassShape, they had to perform it 24 times using EyePassShapes (thus using their eyes).

After five days, the second trial took place. This time each participant was asked to perform her PassShape (by drawing or using the eyes, according to the respective groups). If the PassShape was correct, the trial was over for this participant, if the shape was wrong, it was shown again to the her with the instruction to remember it. Participants from group three had to perform the PassShape again for 24 times using EyePassShapes if they had forgotten it.

The final trial took place after additional five days. The participants were asked a last time to enter their PassShapes. In the end, the participants were asked to fill out a final questionnaire which was used to let the participants rate their memory and find out which memory strategies they used, if any.

7.3 Hypotheses

For the memorability evaluation of EyePassShapes, the following hypotheses have been stated:

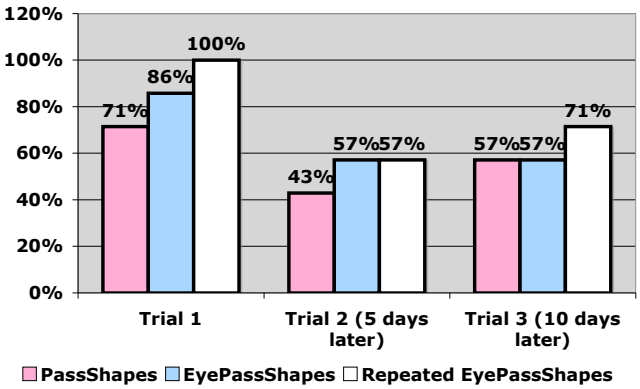


Figure 13: Percentage of recalled PassShapes during the memorability study.

(H6) PassShapes using EyePassShapes are as memorable as PassShapes using the touchpad.

(H7) PassShapes using EyePassShapes with the repeated input strategy are easier to remember than without.

7.4 Participants

The selection of participants for the memorability study was rather tricky due to the high requirements. Participants needed to be available for three consecutive appointments with an intermediate timespan of exactly five days. Out of the possible candidates, 21 volunteers had been selected. Thus, each of the three groups consisted of seven people. None of them had participated in any of the other studies related to PassShapes or EyePassShapes. The average age of the participants was 28 years. The youngest was 24, the oldest 35. Ten were female, eleven were male.

The three groups did not significantly differ in basic demographic data – like education, age, gender and the like – and the rating of their memory skills, which was asked in the first trial.

7.5 Results

Figure 13 shows the correctly recalled PassShapes for the different trials and input strategies. In the first trial, all members of the third group (repeated EyePassShapes) could correctly recall their PassShape while only five out of the seven (71%) members of group one (PassShapes) could remember their PassShape and six out of seven (86%) of group two (EyePassShapes). In the second trial, all groups performed worse. Only four members (57%) of group two and three and less than half of group one could correctly recall their PassShapes. In the last trial after ten days, the biggest recall rate could be found in group three. Five out of seven (71%) of the participants that used repeated EyePassShapes could still remember their PassShape. Only four members of group one and two could successfully recall their PassShapes.

A one-way analysis of variance showed no significance for the differences in the results of the different input strategies (trial 1: $F_{2,18}$=1.13, p=.35; trial 2: $F_{2,18}$=.17, p=.85; trial 3: $F_{2,18}$=.18, p=.84). However – even though the slight advantage of repeated EyePassShapes had no significance – the results showed that EyePassShapes did not perform worse than PassShapes in sense of memory, which supports

hypothesis (H6). Hypothesis (H7) could not be adequately supported and thus had to be rejected.

The evaluation of the questionnaire revealed that only 24% of the participants did not use special strategies to remember the PassShapes. The strategy that has been mentioned mostly was to try to find a meaningful shape within the PassShape like a house or an animal. 33% of the participants said that they used this strategy. Out of the rest, 29% stated that their strategy to remember the PassShape was to remember the movement used to perform it. The remaining 14% used unique strategies. For instance, one of the participants mentioned that the PassShape reminded her of an emotion (*"it's going upwards"*), which she then remembered. Another participant mentioned that it was easy to recall the PassShape once he saw the dotted background of the EyePassShapes prototype. An interesting finding is that none of the members of the group "repeated EyePassShapes" used a unique strategy. This was most probably due to the fact that an effective strategy had already been provided to them. The obvious advantage of the strategy of repeated input is that it is automatically conducted when using the system regularly and does not require abstract memory strategies.

8. DISCUSSING EYEPASSSHAPES

The results of the different evaluations allowed us to re-evaluate the EyePassShapes system with respect to the requirements for authentication systems in public spaces that have been stated in the introduction. The simple question is whether EyePassShapes can fulfill them or not.

A question that is easy to answer is if EyePassShapes would be easy to deploy. The answer is "yes". Standard eye tracking input methods rely on accurate positioning and thus the users need to be calibrated and tracked by the system. This requires expensive hardware. EyePassShapes on the other hand does only require data about relative eye movements. Therefore, low weight and low cost eye trackers are fully satisfying. In the best case, such an eye tracker could be realized by adding a miniature camera to the public terminal which is rather cheap. In most cases, public terminals are already equipped with security cameras – recording the users' faces – that could be exploited for EyePassShapes. The same technology could be used by an attacker. Fortunately, timing of key presses is essential for a successful attack as well, which would require a second camera or sensor.

The second question refers to the memorability of the authentication token. The memorability analysis could not attest improved memorability to EyePassShapes compared to PassShapes. At least we could show that it is as easy to remember as PassShapes, which in previous work [23] has been attested better memorability than standard PINs. Thus, we argue that PassShapes performed with the EyePassShapes system are appropriate authentication tokens for authentication in public spaces.

The question whether EyePassShapes is appropriate in terms of time-critical tasks is harder to answer but at the same time very interesting. The results indicate that this question is directly connected to the question about the security of the system. Firstly, EyePassShapes can be performed very fast. The results of the usability analysis showed that it is as fast as PassShapes or better. However, this is only the case if the one stroke approach is used. That is, the whole shape is performed as one gesture and not accumulatively. Using the accumulative method takes around six times longer in average.

So why not just limit the input to one-stroke authentication? This is when security joins the discussion. The results of the security evaluation revealed the tendency that it is easier for an attacker to steal the PassShape of a user when EyePassShapes is used with the one-stroke approach. Nevertheless, both approaches are significantly more secure than standard PIN or standard PassShapes on a touchpad.

This produces a dilemma: EyePassShapes can either be used the fastest or most secure way, not both at the same time. We think that a possible solution for this problem lies in providing awareness about this fact to the users of the system. Thus, they could decide on the approach depending on the respective situation. In a crowded and busy situation, they could choose to use the faster method while in a quiet and more relaxed situation the more secure method could be applied. It should be added again that in any case EyePassShapes is fully resistant to shoulder surfing attacks.

9. CONCLUSION AND FUTURE WORK

In this paper, we presented EyePassShapes, an authentication system that has been created to fulfill the special requirements of authentication on public terminals. This kind of authentication system should not only be very secure but also easy to use and easy to deploy. Different evaluations showed that EyePassShapes is significantly more secure than PIN-entry – the current standard authentication method for public terminals – and can be performed well and fast. No participant of the user studies had any major difficulties interacting with EyePassShapes.

There are several interesting aspects of EyePassShapes that we would like to answer in the future. One of them being the memorability of multiple PassShapes. That is if users will be able to handle and remember a number of PassShapes for different purposes.

Another very interesting question that is yet to be answered is how interaction with EyePassShapes will change when used on a daily or regular basis. Will users create specific tactics or specific behavior? For instance, it would be interesting to find out whether users actually would change their input strategy in different contexts as proposed in this paper. That is, if they would use the faster one-stroke approach in crowded situations and the more secure accumulative method if there is no time pressure. Another point is if and how users can improve in performance when using EyePassShapes regularly. Informally, we can state that the learning curve of the people working with and on EyePassShapes was rather steep. The time needed for authentication decreased and the comfort in using the system increased drastically over time. It would be worthwhile to investigate this effect more deeply.

10. ACKNOWLEDGMENTS

The authors would like to thank Roman Weiss who significantly contributed to the original concept of EyePassShapes.

11. REFERENCES

[1] A. Bulling, D. Roggen, and G. Tröster. It's in your eyes - towards context-awareness and mobile hci using wearable eog goggles. In *Proc. of the 10th International Conference on Ubiquitous Computing (UbiComp 2008)*, volume 344 of *ACM International*

Conference Proceeding Series, pages 84–93. ACM Press, Sept. 2008.

[2] L. Coventry, A. D. Angeli, and G. Johnson. Usability and biometric verification at the atm interface. In *CHI '03: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 153–160, New York, NY, USA, 2003. ACM.

[3] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud. Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. *Int. J. Hum.-Comput. Stud.*, 63(1-2):128–152, 2005.

[4] A. De Luca, E. von Zezschwitz, and H. Hußmann. Vibrapass - secure authentication based on shared lies. In *CHI '09: 27th ACM SIGCHI Conference on Human Factors in Computing Systems*. ACM, Apr. 2009.

[5] A. De Luca, R. Weiss, and H. Drewes. Evaluation of eye-gaze interaction methods for security enhanced pin-entry. In *OZCHI '07: Proceedings of the 2007 conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: design: activities, artifacts and environments*, pages 199–202, New York, NY, USA, 2007. ACM.

[6] A. De Luca, R. Weiss, H. Hußmann, and X. An. Eyepass - eye-stroke authentication for public terminals. In *CHI '08: CHI '08 extended abstracts on Human factors in computing systems*, pages 3003–3008, New York, NY, USA, 2008. ACM.

[7] T. Deyle and V. Roth. Accessible authentication via tactile pin entry. *Computer Graphics Topics*, Issue 3, Mar. 2006.

[8] R. Dhamija and A. Perrig. Déjà vu: a user study using images for authentication. In *SSYM'00: Proceedings of the 9th conference on USENIX Security Symposium*, pages 4–4, Berkeley, CA, USA, 2000. USENIX Association.

[9] H. Drewes and A. Schmidt. Interacting with the computer using gaze gestures. In *International Conference on Human-Computer Interaction (INTERACT): 11th IFIP TC 13 International Conference*, volume 2, pages 475–488, September 2007.

[10] E. Hayashi, R. Dhamija, N. Christin, and A. Perrig. Use your illusion: secure authentication usable anywhere. In *SOUPS '08: Proceedings of the 4th symposium on Usable privacy and security*, pages 35–45, New York, NY, USA, 2008. ACM.

[11] R. J. Jacob. What you look at is what you get: eye movement-based interaction techniques. In *CHI '90: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 11–18, New York, NY, USA, 1990. ACM.

[12] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd. Reducing shoulder-surfing by using gaze-based password entry. In *SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security*, pages 13–19, New York, NY, USA, 2007. ACM.

[13] B. Malek, M. Orozco, and A. E. Saddik. Novel shoulder-surfing resistant haptic-based graphical password. In *EuroHaptics 2006*, 2006.

[14] W. Moncur and G. Leplâtre. Pictures at the atm: exploring the usability of multiple graphical passwords. In *CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 887–894, New York, NY, USA, 2007. ACM.

[15] S. N. Patel, J. S. Pierce, and G. D. Abowd. A gesture-based authentication scheme for untrusted public terminals. In *UIST '04: Proceedings of the 17th annual ACM symposium on User interface software and technology*, pages 157–160, New York, NY, USA, 2004. ACM.

[16] J. Rogers. Please enter your 4-digit pin. *Financial Services Technology, U.S. Edition*, Issue 4, Mar. 2007.

[17] V. Roth, K. Richter, and R. Freidinger. A pin-entry method resilient against shoulder surfing. In *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security*, pages 236–245, New York, NY, USA, 2004. ACM.

[18] H. Sasamoto, N. Christin, and E. Hayashi. Undercover: authentication usable in front of prying eyes. In *CHI '08: Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, pages 183–192, New York, NY, USA, 2008. ACM.

[19] R. Shadmehr and T. Brashers-krug. Functional stages in the formation of human long-term motor memory. *The Journal of Neuroscience*, 17:409–419, 1997.

[20] L. Standing. Learning 10,000 pictures. *The Quarterly Journal of Experimental Psychology*, 25:203–222, 1973.

[21] D. S. Tan, P. Keyani, and M. Czerwinski. Spy-resistant keyboard: more secure password entry on public touch screen displays. In *OZCHI '05: Proceedings of the 19th conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction*, pages 1–10, 2005.

[22] J. Thorpe, P. C. van Oorschot, and A. Somayaji. Pass-thoughts: authenticating with our minds. In *NSPW '05: Proceedings of the 2005 workshop on New security paradigms*, pages 45–56, New York, NY, USA, 2005. ACM.

[23] R. Weiss and A. De Luca. Passshapes - utilizing stroke based authentication to increase password memorability. In *NordiCHI 2008: Proceedings of the 5th Nordic Conference on Human-Computer Interaction*, pages 383–392, New York, NY, USA, 2008. ACM.

[24] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *AVI '06: Proceedings of the working conference on Advanced visual interfaces*, pages 177–184, New York, NY, USA, 2006. ACM.

[25] J. O. Wobbrock, B. A. Myers, and J. A. Kembel. Edgewrite: a stylus-based text entry method designed for high accuracy and stability of motion. In *UIST '03: Proceedings of the 16th annual ACM symposium on User interface software and technology*, pages 61–70, New York, NY, USA, 2003. ACM.

[26] J. O. Wobbrock, J. Rubinstein, M. W. Sawyer, and A. T. Duchowski. Longitudinal evaluation of discrete consecutive gaze gestures for text entry. In *ETRA '08: Proceedings of the 2008 symposium on Eye tracking research & applications*, pages 11–18, New York, NY, USA, 2008. ACM.