EyePass - Eye-Stroke Authentication for Public Terminals

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

Xueli An
EEMCS
Delft University of Technology
Mekelweg 4
2628 CD Delft, The Netherlands
X.An@ewi.tudelft.nl

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

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

CHI 2008, April 5 – 10, 2008, Florence, Italy
ACM 978-1-60558-012-8/08/04.

Abstract
Authentication on public terminals e.g. on ATMs and ticket vending machines is a common practice. Due to the weaknesses of the traditional authentication approaches PIN and password, it is possible that other people gain access to the authentication information and thus to the users' personal data. This is mainly due to the physical interaction with the terminals, which enables various manipulations on these devices.

In this paper, we present *EyePass*, an authentication mechanism based on PassShape and eye-gestures that has been created to overcome these problems by eliminating the physical connection to the terminals. *EyePass* additionally assists the users by providing easy-to-remember PassShapes instead of PINs or passwords. We present the concept, the prototype and the first evaluations performed. Additionally, the future work on the evaluation is outlined and expected results are discussed.

Keywords
Eye-gestures, authentication, privacy, security.

ACM Classification Keywords
H.5.2 [Information interfaces and presentation (e.g., HCI)]: User Interfaces – Input devices and strategies;

Public Terminal Authentication

While the world becomes more and more connected, services start to be ubiquitously available. Usage of these services often takes place in public spaces and here mostly on public terminals. We use them for withdrawing money, buying plane or train tickets, topping up mobile phone prepaid cards and other purposes. These and other examples show, that a huge amount of conventional services lost their bound to a specific location but became ubiquitous.

These new opportunities imply new challenges. Since most of them require interactions with machines in public spaces, authentication is an important aspect. That is, users have to validate their identity to a machine to be able to use the offered service. This is necessary since they are dealing with highly sensitive user data, e.g. bank account or credit card data.

Unfortunately, the advantage of the ubiquity of public terminals is their weakest point at the same time. They are publicly available, thus to everyone, and the interaction with them happens in a direct physical way. This means that they are exposed to manipulations. When interacting with public terminals, users are in the field of vision of other people, which might lead to additional security problems. A common problem is the manipulation of ATMs to get in possession of users' PINs and so getting access to their bank accounts. The most common attack is called shoulder-surfing and means that an attacker is trying to sneak on the person's PIN by simply looking over his shoulder (directly or with technical means like hidden cameras).

Another problem is that due to the sheer amount of different services that demand authentication, users have to memorize many different passwords and PINs. A short survey we conducted showed that 59 out of 88 participants (55,7%) had already forgotten a PIN with the consequence that their access to a specific service was locked by the service provider. We assume that many humans have problems memorizing abstract number sequences and complex passwords used for current authentication purposes.

To conclude we identify the need for new authentication techniques. On the one hand security must be increased especially regarding the usage in public spaces. On the other hand more memorable authentication tokens would be favorable.

Latest research provided some promising approaches for each of these purposes as shown in the next section. The goal of this work is to develop a new authentication approach combining the advantages in security as well as in memorability.

Alternative Authentication Approaches

The problem of authentication on public terminals as well as the weaknesses of the traditional authentication techniques are not new and have been addressed in different scientific work in a huge variety of potential solutions.

Regarding the memorability problem (and thus the existence of very weak passwords/PINs like birthdays, '0000' etc.) there exist different solutions using graphical passwords. The best known of them is Draw-a-Secret (DAS) [5], that uses shape based passwords. In its different versions it either utilizes a grid or background images to recognize and verify the shapes input by the users. In [9], Wiedenbeck et al. chose a

different approach called PassPoints, in which users authenticate themselves to a system by selecting points on their password image. The evaluation performed by Moncur et al. [7] proofs that multiple graphical passwords are easier to be memorized than multiple PINs.

While these approaches mainly consider improved memorability, others try to enhance the security of authentication. For instance, Kumar et al. evaluated traditional eye-gaze interaction techniques on their appropriateness for PIN entry [6]. Tan et al. [8] tried to increase the security of manual password entry by adapting these input modes.

Of course, biometric authentication methods as discussed in [1] are suitable to handle the memorability problem of traditional authentication as well as to increase security. Nevertheless, there exist some disadvantages: as a physical attribute of a distinct person is used, cases like a grandmother who sends a grandchild to the ATM are not possible anymore. Furthermore, to record and administrate biometric data means a huge effort for the service provider and could lead to privacy concerns of the users.

EyePass: PassShape meets Eye-Gestures

The concept that we are evaluating is a combination of two different technologies: PassShape and Eye-Gestures.

PassShape

The PassShape concept has already been outlined in [2]. It is an alternative authentication method (originally pen-based) that focuses on increased security and is supposed to be easier to memorize compared to traditional authentication mechanisms like PIN or passwords. The idea is that people can more easily remember complex shapes than complex combinations of digits or letters. A PassShape consists of arbitrary combinations of eight basic strokes as shown in Figure 1. The strokes do not have to be connected, which allows the creation of complex shapes and thus, secure authentication tokens.

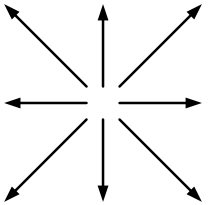

Figure 1: The eight available PassShape strokes.

An example combination is depicted in Figure 2 (left) whereas Figure 2 (right) shows the same combination as a shape that is easy to remember. This means longer shapes can be used as a password, which increases their security while they remain easy for the users to remember.

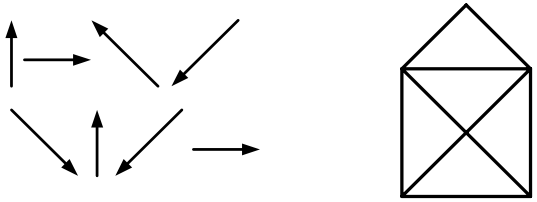

Figure 2: An 8-digit stroke password (left) and an easy-to-remember corresponding (right).

Eye-Gestures

The second concept included in *EyePass* is based upon the interaction technique eye-gestures, developed and evaluated by Drewes et al. in [4]. It enables users of computing systems to invoke commands by moving their eyes in a specific way (drawing patterns with the eyes). Eye-gestures are a novel approach in the research field of eye-tracking. As eye-gaze input methods are resilient against common attacks on PINs, they have recently been evaluated for the usage with ATMs [3]. The eye-gesture approach turns out to be especially suitable for this purpose because of its high resistance against input errors and its very easy deployment in existing hardware (only low-resolution cameras and no calibration process is needed for eye-gestures to work). To enter a specific number using eye-gestures, the user had to perform a gesture imitating the regarding number. For some users it was difficult to perform the right gestures, especially because the gestures for the different digits had to be remembered. Due to this fact entering PINs using eye-gestures took them significantly longer time than traditional PIN input.

EyePass

The concept of *EyePass* now utilizes the stroke recognition ability of the eye-gesture concept and combines it with the stroke based password recognition of PassShape. So users can profit from easy-to-remember graphical passwords provided by the PassShapes and simultaneously use eye gestures as a very secure input technique. Due to the use of PassShapes, the above mentioned disadvantage of having to remember a gesture alphabet does not exist in *EyePass*. Users just have to remember their authentication patterns and can directly input them using eye-gestures.

Since PassShapes only consists of strokes it perfectly fits the biological constraints of the human eye. Eyes move in fast and straight saccades and thus cannot perform any curves or other non-linear shapes.

To summarize, the *EyePass* mechanism works as follows: if users want to input their password (a stroke based shape) to a public terminal, they press a button and hold. At the same time they perform the strokes with their eyes. After finishing that, the button is released and the algorithm checks whether the shape has been input correctly. If yes, access is granted, if not, the process restarts from the beginning.

The main advantage of this approach is the increased security compared to the original PassShape approach because it is very hard for attackers to spy on the users eyes and to gain access to the secret shape. Besides the button press there is no physical contact to the terminal, so manipulations have no or only small effect on the users' security.

At this point it has to be noted that the transfer of the PassShape algorithm to an eye-gesture based version has one disadvantage compared to the original concept. Because it is very hard for humans to perform two strokes in the same direction one after another with their eyes, it is almost impossible to have PassShapes with two or more times of the same stroke in a row.

Prototype

Our prototype consists of an industry standard eye tracker running with a standard Windows PC. We

developed an algorithm that is capable to recognize the strokes performed with the eye by analyzing the fixations and the saccades that have been made. So it can match the recognized strokes against the abstract representation of the PassShape in the authentication database. While performing the PassShape gesture the users hold the space bar pressed to indicate that they are trying to enter an authentication token. This is necessary as it is impossible for humans eyes to stop moving, which would lead to a huge amount of unintended recognized strokes. For security and usability reasons, no feedback is provided to the users.

Preliminary Memory Study

In order to prove the better memorability of PassShapes compared to classical PINs we performed a preliminary experiment with 55 students of our faculty. One group tested the memorability of the PassShape patterns. Each participant was presented a random shape consisting of five strokes and was told to enter it on a tablet PC with a stylus. To avoid demand characteristics we did not reveal the true intention of the experiment to the participants and masked it as an experiment trying to evaluate different touch based input methods. The other group was shown a four-digit-PIN, which they had to enter on another tablet PC using a stylus as well. Three days later the volunteers were asked in an email if they could still remember the shape respectively the PIN they had entered during the study. The results show that 85% of the participants that had entered a shape in the experiment could still recall that shape while only 60% of the subjects in the PIN group could remember it. Although we have to admit that the masking of the experiment did not work as well as expected in some cases and that there was no control of extraneous variables, the results indicate statistic significance and give preliminary proof of the increased memorability of PassShapes compared to PINs. In future work we will conduct more elaborate studies in this field.

Security Analysis

As shown in [6] and [3] eye-gaze based input methods are resilient against most of the attacks regarding fraud in conjunction with public terminals (despites video surveillance of the eyes). Due to the fact that only little physical contact is necessary for interaction and the obvious difficulty in monitoring and evaluating the users' eye movements, common scenarios like shoulder-surfing or public terminals with manipulated or video-surveilled number pads cannot be successful any more. Additionally, using the PassShape concept enables the use of more complex authentication tokens, which leads to a further increased security.

EyePass Future Evaluations

With the previously explained prototype, we plan to evaluate *EyePass* on different aspects. This includes its usability as well as its memorability. An important question is whether *EyePass* significantly increases the ease of use of eye-gestures for authentication (e.g. compared to the PIN entry approach outlined in [3]).

The main problem of the existing approaches of eye-gestures is the memorability of big sets of commands. Since every action needs a unique gesture, the users have to remember a big amount of them. Fortunately, *EyePass* users have to remember only one shape (or one per terminal to increase security), which will authenticate them. That is, we consider eye-gestures and thus EyePass to be an effective mechanism for the task of authentication with public terminals.

Regarding the question of usability, we are planning to conduct a user study at our premises. We will let the participants use a PIN entry method based on plain eye-gestures as well as *EyePass* to compare these two approaches. Furthermore, we are planning to evaluate *EyePass* against PassShape since we assume that it will be slower in use.

The memorability evaluation will be based on the ability to remember a PassShape instead of a PIN code. This evaluation will be based on the lessons learned during the preliminary memorability evaluation as outlined earlier in this paper. Another point we want to evaluate is whether PassShapes entered by a stylus or entered with the eyes show any difference in memorability.

Conclusion

In this paper, we discussed *EyePass*, a novel authentication mechanism for public terminals, which is based on PassShape, a concept to increase memorability of authentication tokens and eye-gestures, a new eye-gaze interaction technique. Combining these two approaches, *EyePass* is an authentication concept, which is easy to use, has high resistance to common attacks on interaction with public terminals and offers enhanced memorability compared to traditional methods.

While in first evaluations we could preliminarily proof the memorability and security advantages of the concept, we are planning to increase these examinations in future work.

Acknowledgements

This work is partially supported by the European Union, in the framework of the FP6 – IST Project DISCREET.

References

[1] Coventry, L., De Angeli, A., and Johnson, G. Usability and biometric verification at the ATM interface. In: Proceedings of CHI '03, Fort Lauderdale, Florida, USA, April 5 - 10, 2003.

[2] De Luca, A., Weiss, R., Hußmann, H. PassShape – Stroke Based Shape Passwords. In: Proceedings of OZCHI 2007, Adelaide, Australia, 28 – 30.11.2007.

[3] 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.

[4] Drewes, H., Schmidt, A. Interacting with the Computer using Gaze Gestures. In: Proceedings of Interact'07. Rio de Janeiro, Brazil. September 10 – 12, 2007.

[5] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. Rubin, A. The design and analysis of graphical passwords. In: Proceedings of USENIX Security Symposium. August 1999.

[6] Kumar, M., Garfinkel, T., Boneh, D., Winograd, T. 2007. Reducing Shoulder-surfing by Using Gaze-based Password Entry. In: Proceedings of SOUPS '07, Pittsburgh, USA, July 18 - 20, 2007.

[7] Moncur, W. and Leplâtre, G. Pictures at the ATM: exploring the usability of multiple graphical passwords. In: Proceedings of CHI '07, San Jose, California, USA, April 28 - May 03, 2007.

[8] Tan, D. S., Keyani, P., and Czerwinski, M. 2005. Spy-resistant keyboard: more secure password entry on public touch screen displays. In: Proceedings of OZCHI'05, Canberra, Australia, November 21 - 25, 2005.

[9] Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., Memon, N. Authentication using graphical passwords: Basic Results. In: Proceedings of Human-Computer Interaction International (HCII 2005), Las Vegas, Nevada, USA, July 22-27, 2005.