PassShape – Stroke based Shape Passwords

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

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

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

ABSTRACT
Authentication today mostly means using passwords or personal identification numbers (PINs). The average user has to remember an increasing amount of PINs and passwords. But unfortunately, humans have limited capabilities in remembering abstract alphanumeric sequences. Thus, many people either forget them or use very simple ones that imply several security risks. In our previous work on PIN entry on ATMs (cash machines), we found out that many persons support their memory recalling PINs by using an imaginary shape overlaid on the number pad. In this paper, we introduce PassShape, a shape based authentication mechanism. We argue that using shapes will allow more complex and more secure authentication with a lower cognitive load. That is, it enables people to use easy to remember but complex authentication patterns.

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.

Keywords
Authentication, Security, Shape Passwords, PassShape.

1. SECURE PASSWORDS AND MEMORY
Nowadays, people are exposed to a wide variety of different services caused by the rapid advances in technology. Most of us are carrying mobile phones, PDAs, notebooks and the like, are using dozens of different internet services, use credit or bank cards for payment, etc. As most services enable access to critical private data (e.g. control over a person's bank account), authentication mechanisms become more and more a critical issue in everyday life. The most common solution for this problem are traditional passwords (combinations of letters, numbers etc.) or PINs (a sequence of numbers). Consequently, one has to remember a huge amount of them.

That is, when talking about authentication, not only security and privacy aspects have to be considered, but also the question of complexity. The higher complexity of a password or a PIN increases its security, but it simultaneously increases the effort to remember it. In a preliminary online survey with 86 participants we confirmed our assumption that many persons forget their PINs from time to time. In that survey, 48 participants (55%) noted that they already forgot their PIN at least once. 64 participants (74%) usually change their PIN number if possible. When asked for the reason, almost all of them answered that they would prefer some numbers that are easier to remember. The limited capability of humans in memorizing abstract alphanumeric sequences seems to be a main issue dealing with authentication methods.

In this work, we argue that there is a correlation between the security and the memorability of common passwords and PIN numbers. Thus, we will introduce PassShape, a shape based authentication method that in our opinion provides easy to remember passwords, but retains and possibly increases the security of complex traditional passwords. Instead of the typical passwords or PINs, PassShape uses user-defined shapes for authentication with a service or the like.

There exist various approaches that focus on graphical passwords and try to enhance the security as well as the usability of authentication mechanisms. Jermyn et al. provide a method called Draw-a-Secret [4] which allows drawings on a grid being used as an authentication token. This fundamental work has recently been extended by [8], who add background images to the grid in order to improve usability.

Other recent work in the field of authentication focuses on increasing the security of the traditional input methods for PINs or passwords. They try to overcome the security threats caused by the simplicity of these methods. An example is the work of Kumar et al. [1], in which they use eye tracking for the input of passwords to provide security against shoulder-surfing, the most common attack on cash cards [5]. This is a serious attack on short and thus easy to spy-on 4-digit PINs. Other work that tries to make PIN entry resilient against shoulder surfing has been done by Roth et al. [6] based on a binary input method for numbers and by Tan et al. [7] that created a spy-resistant keyboard. We suppose that our approach has the potential to increase the security against such attacks as well. It allows longer and thus harder to spy-on stroke sequences that remain easy to remember for the users that have a specific figure in mind.

2. PassShape CONCEPT
PassShape is based on observations, which we made during the evaluation of different PIN entry methods for standard ATMs (cash machines). We noticed that many people remember their PINs not as a combination of numbers but as a shape on the number pad of the ATM. This finding has been supported by the previously mentioned online survey. Users reported that they build an overlying shape by connecting the single digits and then memorize only this geometrical figure or at least use it for supporting their memory. Figure 1 (left) depicts the typical layout of an ATM number pad and the shape (a triangle) used

OzCHI 2007 Proceedings, ISBN 978-1-59593-872-5

to remember the exemplary number sequence 7197. Assuming this, it seems reasonable to replace the numbers with their shape representation, eliminate the PIN itself and utilize the shape alone for authentication purposes. Thus, we developed a new authentication method based on shapes, which allows complex (more secure) but easy to remember passwords.

The idea is to use shapes as passwords instead of the common approaches. In this concept, a shape can consist of an unlimited amount of horizontal, vertical and diagonal strokes. Figure 1 (right) shows all eight possible strokes used in our approach.

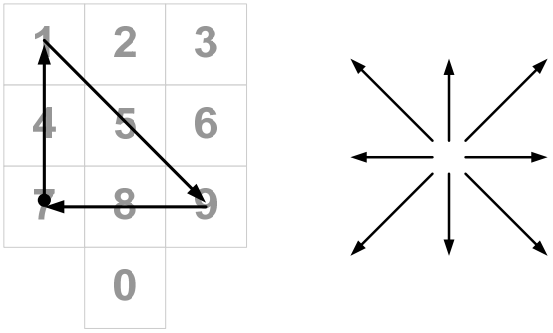

Figure 1: A shape to remember the PIN 7197 (left) and the eight possible strokes (right) of the concept.

For the recognition of a shape password, the strokes do not have to be connected, which in consequence means that an unlimited amount of stroke combinations is possible. That is, a shape password can consist of several single shapes (e.g. a triangle followed by a square). For the algorithm, the position of the strokes is not relevant, but just the sequential order of the used strokes. Nevertheless, for the users, the position and layout is of great importance since building specific shapes out of the strokes will help him to remember the password, even if it is complex.

Figure 2 exemplarily shows a sequence of strokes as interpreted by the algorithm and the corresponding shape memorized by the user. On the left side, a hard to remember sequence of strokes is depicted, while on the right side, the same combination is presented as an easy to remember shape.

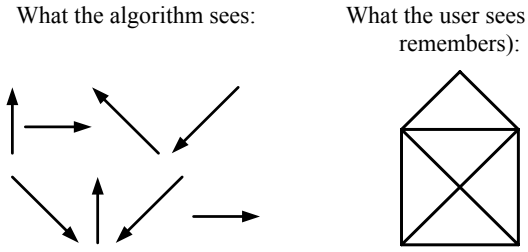

Figure 2: An 8-digit stroke password (left) and the corresponding shape to remember it (right).

3. VALIDATION APPROACH AND WORK IN PROGESS

As mentioned before, we firstly conducted a preliminary online survey with 86 participants. More then 40% stated that they use geometrical patterns on the number pad to remember their PINs. The need to improve the memorability of authentication mechanisms is encouraged by the finding that over 55% of the participants reported that they had already forgotten their PIN number at least once, even though typical number sequences consist of only four digits. This is the reason why 74% of them usually change their PIN to an easier one like their birth date, which bears serious security risks. A short outline of the PassShape concept raised interest in 50% of the participants.

In future work we will at first try to verify the benefits in memorability provided by the shape based authentication. For this purpose, a long time study is planned to compare the memorability of PINs to shape passwords. Another study will deal with the usability of the PassShape concept focusing on ease of use, error-proneness, interaction speed and acceptance by the users. Additionally, we plan to evaluate security issues of this new concept. For instance, we need to investigate whether people will use extremely simple or well-known shapes, which could be a security risk. Accordingly, it might be necessary to set specific requirements for the definition of shape passwords (e.g. an appropriate minimum number of strokes). As stated, we believe that this approach has the potential to increase security of authentication against common attacks like shoulder surfing, which is also to be investigated within this work.

We plan the implementation of PassShape using two different interaction techniques. Firstly, a pen or touch screen based input implementation and secondly a security-enhanced version based on the gaze gestures concept, introduced in [3]. For this method, the movement of the users' eyes is used to recognize specific strokes. Thus, this approach is resilient against shoulder surfing as other gaze based interaction techniques as explained in [1] and [2], which raises its security.

4. ACKNOWLEDGMENTS

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

5. REFERENCES

[1] 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.

[2] De Luca, A.,Weiss, R., Drewes. H. Evaluation of Eye-Gaze Interaction Methods for Security Enhanced PIN-Entry. To appear in proceedings of OZCHI 2007, Adelaide, Australia, 28.-30.11.2007.

[3] Drewes, H., Schmidt, A. Interacting with the Computer using Gaze Gestures. In: Proceedings of Interact'07. Rio De Janeiro, Brasil. September 10 – 14, 2007.

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

[5] Rogers, J. 2007. "Please enter your 4-digit PIN". In *Financial Services Technology,U.S. Edition*, Issue 4, March 2007.

[6] Roth, V., Richter, K., and Freidinger, R. 2004. A PIN-entry method resilient against shoulder surfing. In: Proceedings of CCS'04, Washington DC, USA, October 25 - 29, 2004.

[7] 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.

[8] Yan, J., Dunphy, P. 2007. Do Background Images Improve "Draw a Secret" Graphical Passwords? To appear in: proceedings of CCS'07, Alexandria, USA. 2007.