Picassopass: a Password Scheme Using a Dynamically Layered Combination of Graphical Elements

Wouter van Eekelen
NHTV Breda University of Applied Sciences
Mgr. Hopmansstraat 1
4817JT Breda, The Netherlands
wouter@picassopass.com

John van den Elst
NHTV Breda University of Applied Sciences
Mgr. Hopmansstraat 1
4817JT Breda, The Netherlands
elst.j@nhtv.nl

Vassilis-Javed Khan
NHTV Breda University of Applied Sciences
Mgr. Hopmansstraat 1
4817JT Breda, The Netherlands
khan.j@nhtv.nl

CHI 2013 Extended Abstracts, April 27–May 2, 2013, Paris, France.
ACM 978-1-4503-1952-2/13/04.

Abstract
In this paper a new graphical password scheme is presented using a dynamic layered combination of graphical elements. It has unique capabilities in terms of low memory burden due to a story based approach, while at the same time being very resistant to shoulder surfing threats. The results of a security evaluation confirm shoulder surfing resistance.

Author Keywords
Graphical password schemes; classification; evaluation; layering; PicassoPass; combination of graphical elements; shoulder surfing

ACM Classification Keywords
D.4.6 [**Security and Protection**]: Authentication; H.5.2 [**User Interfaces**]: Evaluation/methodology; H.5.2 [**User Interfaces**]: Graphical user interfaces (GUI); H.5.2 [**User Interfaces**]: Theory and methods; K.6.5 [**Security and Protection**]: Authentication

Introduction
People are using passwords every day, multiple times; for online banking accounts, for social network profiles and to check their webmail from work. The great majority of all these digital systems have security measurements based on textual passwords. For over a decade the textual

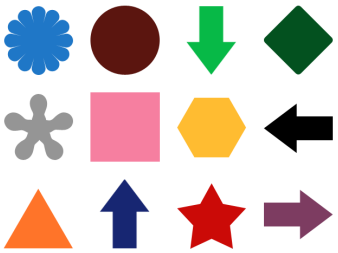

Figure 1: Two out of five potential layers that *PicassoPass* supports

passwords' shortcomings have been documented [15]. A solution that has been proposed to those shortcomings is using graphical passwords [11, 4], which are based on graphics, images, shapes and colors instead of text.

Nevertheless, after all these years, despite the demonstrated benefits, graphical passwords have failed to replace textual passwords [3]. While textual passwords are mainly designed to serve technical goals first, graphical passwords are mainly designed to serve user goals first [6]. This approach has considerable advantages, but also raises challenges. Graphical passwords are more difficult to implement due to complex human factors that have to be considered [12].

In this paper *PicassoPass* is presented, a novel solution in graphical passwords. Both its advantages and shortcomings are listed and the results of a shoulder surfing attack security evaluation are presented.

Combining graphical elements for cued recognition

As described by [12], [2] and [8], graphical password schemes can be based on recall (like making a drawing), recognition (like finding spots on an image), cued recall or cued recognition. This paper focuses on graphical password systems using cued recognition, where the idea is that people have to retrieve objects from memory by mentally revisiting locations or stories, "where the story or the semantic relationship between the images assists the user in the recognition of password images" [8].

Typically the used images or graphical elements that are being displayed are positioned within a grid [12, 2] instead of being combined. The main reason is likely that combining them increases complexity for the user, although most of the time it also increases the strength of the password and the theoretical password space, thus enhancing security.

A well known example of a graphical password scheme that combines graphical elements is Passfaces [17, 6, 19, 2, 13]. Passfaces displays nine different images, limiting the password space to 9^N (N is the number of password images). If graphical elements are combined, especially in a dynamic manner, the password space could be extended.

The best approach would be giving users a limited amount of clickable choices, while at the same time they have more possibilities. Layering could provide such approach: an image is constructed out of different layers. One layer could be for example a shape and another layer the color, as illustrated in figure 1. If a generated image has for example 12 different clickable choices and for each choice a shape and a color are combined, then it would result in a password space of 24 for a single image.

A color and a shape are two different things that humans can distinguish. So it doesn't matter that they are combined, they could also be presented uncombined so the image would have 24 different clickable choices with only a shape or color. When users know they need to select the correct color, they can mentally filter the other information and ignore what they don't need, like shapes. If someone would look over the shoulder, he/she only sees that the user selects for example a red star. But was it selected because of the color red or because it was a star shape? Adding more layers will complicate things more for shoulder surfers, especially if every time the combination of layers is different (dynamic).

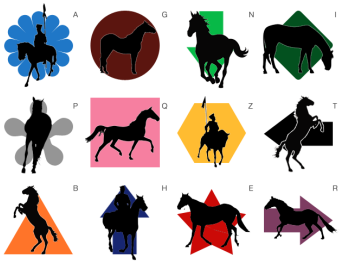

Figure 2: A screenshot of a complete *PicassoPass* password scheme

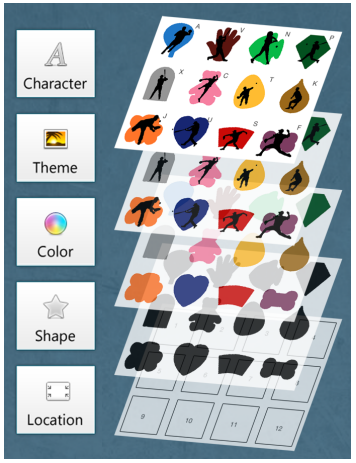

Figure 3: Five layers that *PicassoPass* supports. Starting from the bottom layer, the location of a certain element, to the top layer, a character displayed on the top right side of the element.

PicassoPass

PicassoPass is a challenge-response based graphical password system. It dynamically combines graphical elements in different layers, which hasn't been described previously. *PicassoPass* uses the combination of graphical elements for a mnemonic approach [8]: a story assists the user in the recognition of graphical elements.

During login, *PicassoPass* presents a sequence of grid-based images. This is called a 'challenge'. The task for the user is to select the correct cell from the grid at each step. What the correct cell is, depends on what the user has chosen as correct when creating the password.

Graphics

In *PicassoPass* each cell is a (random) layered combination of four different things: a basic shape (for example square or triangle), a color, a character from the alphabet and a shape based on a theme. This is presented in figure 2.

Instead of presenting a grid of 60 elements, the layering makes it possible to display a grid with only 12 elements, which needs less space on screen and at the same time inhibits shoulder-surfing. When a user logs in, an attacker would not know why the user has selected a cell, since there are five different possible reasons (the four mentioned earlier, together with the position of the correct cell in the grid, see figure 3). It would require multiple captures of the login process to rule out all potential reasons.

With every login the elements are randomly combined. For every grid/step, the user choses what selector is used, like the shapes, character, color or the position of the cell. The user is going through each grid one by one until he/she is has finished the challenge manually. An example could be that with the first grid, red is correct, the second top left position and at the third grid the circle is correct and the user finishes the challenge.

Memory

The impact on memory and the ability to remember a password is called memory burden: how much does a user have to remember so that she is able to input the password correctly in one attempt [2]. There are different techniques that can help to lower the memory burden [6, 4, 2], or limit the number of steps, of which the latter will also lower the strength of a password.

PicassoPass uses cued recognition with a story approach. A positive effect of the story approach used in *PicassoPass* is that it contributes to a better recalling of a password: when the items or objects that need to be remembered can be associated with something concrete [20], they will be easier to remember [18]. The storage of the image in the long-term memory is not based on storing the actual image itself, but instead a 'meaningful interpretation' as described in 1977 by Mandler & Ritchey [10]. At the same time, there is a preference for images that are symmetric so memory load can be reduced [14, 11].

To aid users of *PicassoPass* with remembering their password, the theme shapes can be used to create a mnemonic story. An example could be 'the blue horse jumped over the green car'. Every underlined word could potentially be a grid/step. To make the above example even stronger, it could be appended with 'that has a yellow star on top'. Although we expect *PicassoPass* to be effective in recall, this paper will not evaluate that aspect.

Technical

PicassoPass can be used on multiple platforms, since the 60 different elements are positioned within a grid of 12

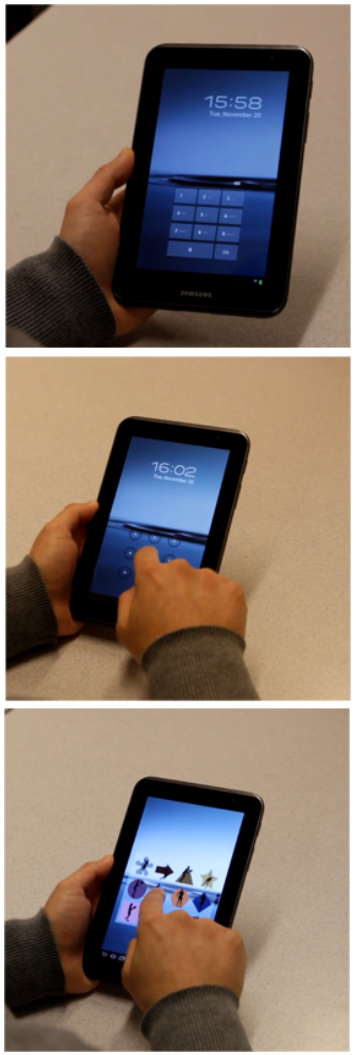

Figure 4: Screenshots of survey videos

elements. A prototype was made for mobile devices with a small screen resolution of 320 pixels width and 450 pixels height and the elements (including the theme shapes) are still distinctive enough.

Complexity
The theoretical password space of *PicassoPass* is higher than (four digit) PIN-based password systems, yet lower than textual passwords with a length of five alphanumeric characters. For each grid, there are 12 distinct locations with each cell having four different elements combined: color, shape, theme and an alphabetic character. So, the possible combinations of each individual grid is 12x5 = 60. If the graphical password has four grids, it would be 60^4, or 12,960,000 possible combinations. A PIN of four digits has (10^4) 10,000 possibilities while a textual password with five alphanumeric characters including upper- and lowercase and symbols has (94^5) 7,339,040,224 possibilities, which is an enormous difference with the four digit PIN code.

Security
A very often discussed threat is shoulder surfing. Shoulder surfing is a capturing attack, in which someone tries to look over the shoulder to capture the password [2]. This can be achieved with recording devices like camera's [2], but also by using keyloggers, screenscrapers (to see what is happening on screen) and mouseloggers [16, 9].

A technique to counter shoulder surfing is the use of decoys [5] so malicious users are confused or cannot detect the correct answer unless they capture multiple trials of the login sequence.

The better the distinction is between colors, shapes and images, the less mistakes users make during input [1, 5], however it also increases the risks on dictionary and shoulder surfing attacks.

Although a significant advantage for memory burden and reducing mistakes, the drawback of a story based approach with clear and distinct colors, shapes and images is that shoulder surfing becomes easier.

PicassoPass proposes a possible solution against shoulder surfing while at the same time benefiting from a mnemonic approach: dynamically combining graphical elements.

Shoulder surfing security evaluation

To test resistance for shoulder surfing an online survey was conducted. 57 participants responded out of 120 sent invitations. The only requirement for participation was perfect (or corrected) vision. No additional demographic information was recorded. Each participant was shown one video of someone entering a password on a tablet device, filmed as the viewer was watching over the shoulder. Participants were divided into three groups. For each group, the used password technique was different. One group of participants saw a numeric password, another group saw a gesture and a third group saw *PicassoPass* (see figure 4). Participants were then asked: "What was the password the user inserted?". After viewing the video, the participant had to select the correct answer from a set of six possibilities.

For example, in the case of the numeric password, the video depicted a user tapping the "2998" numeric code to unlock the tablet. After viewing this short video, participants were asked the question: "What was the password the user inserted?". Participants got the following six options to choose from: "0987", "1234", "8463", "2998", "2292", "3015". These options were

randomly ordered for each participant. Similarly, in the case of the gesture password, participants, after viewing the video with the user unlocking the tablet with a gesture, were asked the question: "What was the password the user inserted?". Participants then saw six images each depicting a possible gesture with the help of an arrow-line. Finally, in the case of *PicassoPass*, the video depicted a user going through three screens of *PicassoPass* to unlock the tablet. Then, participants got six options of possible element combinations to choose from.

	Shoulder attack	
Interface	Successful	Unsuccessful
Numeric	17	1
Gesture	13	4
PicassoPass	0	22

Table 1: Survey results

In total there were 57 participants (numeric: 18, gesture: 17, PicassoPass: 22). The null hypothesis was H0: the three password methods would not have any effect in preventing shoulder surfing attacks. The two variables were: v1: password technique, v2: shoulder surfing attack. Both of them are nominal with possible values: v1=[Numeric, Gesture, PicassoPass] and v2=[successful, unsuccessful]. Since at least one of the cells of the contingency table is less than 5, the statistical test needed to test the hypothesis is the "Fischer exact probability test" [7]. The result is that the exact probability of the H0 being true is practically 0, actually: 5.83^{-12}. That means the H0 can be rejected. By having a look at the contingency table it is clear that *PicassoPass* is significantly superior to the two existing password insertion methods.

The results of this between-subject study design show that none of the 22 participants who were assigned to *PicassoPass* correctly guessed the password, while almost everybody correctly guessed the numeric password (see table 1). This confirms the potential of *PicassoPass* to protect from shoulder surfing attacks.

Conclusions and future work

PicassoPass is a challenge-response based graphical password system that uses cued recognition. Its novelty is that it dynamically combines graphical elements in different layers, which has not been tried out previously. The main hypothesis was that *PicassoPass* has an increased shoulder surfing resistance due to layering of graphical elements. This has been evaluated and confirmed.

To make this work more complete, other types of attacks such as password guessing and resetting need to be evaluated. Future studies will also focus on usability aspects of *PicassoPass* and memory burden.

References

[1] Angeli, A. D., Coventry, L., Johnson, G., and Renaud, K. Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies* (2005).

[2] Biddle, R., Chiasson, S., and van Oorschot, P. Graphical passwords: learning from the first twelve years. Tech. rep., School of Computer Science, Carleton University, 2011.

[3] Chiasson, S., and et al. A second look at the usability of click-based graphical passwords. In *ACM SOUPS*, Press (2007), 1–12.

[4] Chiasson, S., Oorschot, P. C. V., and Biddle, R. Graphical password authentication using cued click-points. In *12 th European Symposium On Research In Computer Security (ESORICS), 2007*, Springer-Verlag (2007).

[5] De Angeli, A., Coventry, L., Johnson, G., and Renaud, K. Evaluating the usability and security of a graphical one-time pin system. In *International Journal of Human-Computer Studies*, vol. 63 (2005).

[6] Gkarafli, S., and Economides, A. Comparing the proof by knowledge authentication techniques. In *International Journal of Computer Science and Security*, vol. 4 (2010), 237–255.

[7] Howitt, D., and Cramer, D. *Introduction to statistics in psychology, 5th ed.* Prentice Hall, Essex, 2011.

[8] Khot, R. A., Srinathan, K., and Kumaraguru, P. Marasim: a novel jigsaw based authentication scheme using tagging. In *Proceedings of the 2011 annual conference on Human factors in computing systems*, CHI '11, ACM (2011), 2605–2614.

[9] Kumar, M., Garfinkel, T., Boneh, D., and Winograd, T. Reducing shoulder-surfing by using gaze-based password entry, 2007.

[10] Mandler, J., and Ritchey, G. Long-term memory for pictures. *Journal of Experimental Psychology: Human Learning and Memory 3* (1977), 386–396.

[11] Nali, D., and Thorpe, J. Analyzing user choice in graphical passwords. Tech. rep., School of Computer Science, Carleton University, Canada, 2004.

[12] Suo, X., Direction, U., Zhu, Y., Suo, X., and Suo, X. A design and analysis of graphical password, 2006.

[13] Tao, H. Pass-go, a new graphical password scheme, 2006.

[14] Thorpe, J., and van Oorschot, P. Graphical dictionaries and the memorable space of graphical passwords. In *Proceedings of the 13th USENIX Security Symposium* (2004).

[15] Thorpe, J., and van Oorschot, P. Towards secure design choices for implementing graphical passwords, 2004.

[16] Thorpe, J., and van Oorschot, P. Human-seeded attacks and exploiting hot-spots in graphical passwords. In *Proceedings of the 16th USENIX Security Symposium* (2007).

[17] Wiedenbeck, S., Waters, J., Brodskiy, A., and Memon, N. Authentication using graphical passwords: Effects of tolerance and image choice. In *In First Symposium on Usable Privacy and Security (SOUPS 2005)*, ACM Press (2005), 1–12.

[18] Wiedenbeck, S., Waters, J., camille Birget, J., Brodskiy, A., and Memon, N. Passpoints: Design and longitudinal evaluation of a graphical password system, 2005.

[19] Wiedenbeck, S., Waters, J., Sobrado, L., and Birgit, J. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the advanced visual interfaces symposium* (2006).

[20] Zin, L., Sun, Q., and Giusto, D. An association-based graphical password design resistant to shoulder-surfing attack. In *Proceedings of the IEEE international conference on multimedia and expo* (2005), 245–248.