Dynamic layering graphical elements for graphical password schemes: creating the difference

chi sparks 2014

Dynamic Layering Graphical Elements For Graphical Password Schemes

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

ABSTRACT

Based on a systematic review of 35 graphical password schemes, in this article a new classification and evaluation framework is proposed. When positioning existing schemes in this framework a novelty is discovered that wasn't previously described: a dynamic layered combination of graphical elements. Given this insight, a new graphical password scheme is created (*PicassoPass*). Positioned against other password systems, it has the potential to perform better on the combination of low memory burden and resistance to shoulder surfing attacks. A security analysis confirms its shoulder surfing resistance.

Author Keywords

Graphical password schemes; classification; evaluation; layering; *PicassoPass*; combination of graphical elements, shoulder surfing.

ACM Classification Keywords

H.5.2 [User Interfaces]: Evaluation/methodology; H.5.2 [User Interfaces]: Theory and methods; D.4.6 [Security and Protection]: Authentication; K.6.5 [Management of Computing and Information Systems]: Security and Protection.

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 passwords' shortcomings have been documented [17]. One solution to these shortcomings is using graphical passwords [7, 13].

A definition of graphical passwords would be: `In a graphical password system, a user needs to choose memorable locations in an image. Choosing memorable locations depends on the nature of the image itself and the specific sequence of click locations` [20].

Scientists have looked into the possibility of graphical passwords, proposing numerous new ideas and systems [3]. Nevertheless, after all these years, despite the demonstrated benefits, graphical passwords have failed to replace textual passwords [6]. While textual passwords are mainly designed to serve technical goals first, graphical passwords are mainly designed to serve user goals first [10]. Such an 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 [14].

Graphical password schemes can be grouped and differentiated within four different underlying ideas. As described by [14], [3] and [11], graphical password schemes are based on recall, recognition, cued recall or cued recognition. An alternative distinction between different types of graphical password schemes is `Cognometrics, Locimetrics and Drawmetrics' [1].

Although very useful, these classifications of graphical password schemes are limited when it comes to pertinent characteristics for design and development, such as security, technical aspects and graphical aspects. In this paper we expand aforementioned classifications of graphical passwords after having reviewed 35 password schemes. The contribution of this classification is an extensive evaluation matrix for designers and developers of graphical passwords. We strongly believe that such an evaluation matrix can help designers position their ideas and to serve as inspiration for novel solutions. To demonstrate this, we present an analysis resulting in a new graphical password solution which we call *PicassoPass*.

This paper is organized as follows. First we present the new classification and evaluation framework. Then we describe *PicassoPass*, a newly identified solution for graphical passwords. In order to contrast it against other systems, the advantages and shortcomings of *PicassoPass* are listed according to the new framework, and finally, the results of a study for shoulder surfing resistance are presented.

CLASSIFICATION AND EVALUATION OF GRAPHICAL PASSWORD SCHEMES

As described by [14], [3] and [11], graphical password schemes can be based on recall, recognition, cued recall or

Published in: van Leeuwen, JP, Stappers, PJ, Lamers, MH, Thissen, MJMR (Eds.) *Creating the Difference: Proceedings of the Chi Sparks 2014 Conference*, April 3, 2014, The Hague, The Netherlands.

cued recognition, or alternatively on `Cognometrics, Locimetrics and Drawmetrics' [1].

Recall is concerned with retrieving the correct answer from memory. Textual passwords work in the same way: the only thing users see is an empty input text field for which they need to recall the correct password. Most recall-based graphical password systems are the ones that require the user to draw something, usually on a grid [5]. Such a solution is also known as Drawmetrics [1].

In the case of cued recall, users have to find previously chosen spots from an image or picture [20]. An example of a cued recall based system is Pass-Go, which uses the game board structure of the game `Go'. By positioning the playing pieces, users can draw their password [15]. Cued recall is essentially a combination of recall and recognition.

Recognition based graphical systems work with a given image or collection of images (mostly displayed in a grid) at which users have to select (by recognizing) the correct spots or images, sometimes in a particular order [7, 9]. This is also called Cognometric [1]. Cued recall uses the given image but gives less cues as compared to recognition.

A final variant of graphical password systems found in literature, is Logimetric. As [1] describe it is `based on the method of loci, an old and well-known mnemonic`. The idea is that people have to retrieve objects from memory by mentally revisiting locations or stories. In a sense it is somewhat the same as cued recognition. An example of a Logimetric graphical password system is Story Scheme as mentioned by [11] `where the story or the semantic relationship between the images assists the user in the recognition of password images`.

We expanded above categories of graphical passwords into a new classification framework. Based on 40 different scientific publications (of which only a selection is referred to in this paper) covering 35 graphical password schemes, we identified a set of variables which can be used to classify and evaluate graphical password schemes. The used publications each describe one or more graphical password schemes. Some of them are the original, first papers on a specific scheme, while others reviewed similar schemes without mentioning a new scheme.

The information extracted from each publication was the name of the password scheme, a short description of the scheme and a list of its features. Given the identified variables and the 35 graphical password schemes we created a new classification framework. Regarding the password schemes and their particular characteristics, the complete set of variables identified in literature was aggregated into five main categories. Each category has one or more variables, on which a scheme was scored or for which was described how that scheme works. We do want to acknowledge that, although we did have a systematic process in categorizing the reviewed schemes, the process still remains to some extent subjective. Nevertheless, we strongly believe that such a classification can provide new perspectives to developers of new schemes and therefore want to contribute it to the community.

CATEGORIES AND VARIABLES

Our new classification and evaluation framework is presented in the form of a matrix comparing password schemes. The resulting matrix contains five `high level` categories: Memory, Complexity, Technical, Security and Graphical. Each category has multiple scaled variables, like password space for Complexity, combining graphics for Graphical, shoulder surfing resistant for Security, password storage for Technical and many more.

A simplified version of the evaluation matrix is presented in Table 1. This matrix contains all the identified categories and variables, but only shows the comparison between *PicassoPass* (which is introduced later in the paper) and a selection of other graphical password schemes. The main reason why those graphical passwords presented in this simplified matrix were selected, is that together they represent the full diversity of graphical passwords. The full list of all 35 graphical schemes that were evaluated is presented in Appendix A. Although all these schemes have been included in our investigation, due to space limitations only a selection of the matrix could be displayed. On request the authors can provide the complete matrix.

Memory

The first category is Memory, which is concerned with the underlying concept of a password scheme and how well it enables users to (easily) remember their passwords. For this purpose a password can be based on the variables mentioned earlier in this paper: recall, recognition, cued recall or cued recognition [3, 11, 14], as well as on Cognometrics, Locimetrics and Drawmetrics [1].

The second aspect of Memory is whether a user can create her/his own password or the password is generated by the scheme. User-created passwords are more likely to be remembered, while system generated passwords are often stronger and less likely to be guessed [3, 11]. A third possibility is that users, instead of creating their passwords, are selecting a password from a (proposed) collection provided by the scheme. This balances the forces between creating and generating passwords [2].

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 [3]. There are different techniques that can help to lower the memory burden [3, 7, 10], or limit the number of steps, of which the latter will also lower the strength of a password.

Using decoys that are (very) similar could have a negative effect on the memory burden, since users have to put more effort in remembering the correct image due to similarities and a higher chance that the wrong image is selected.

	Graphical Password System / Elements of (technical) design	Textual	PicassoPass	Pass Faces	Color Login	Déjà Vu	MARASIM	V-GO	GrIDsure	Pass Doodle	Patternlock	Inkblots	Story Scheme	Pass shapes
Memory	1: Recall 2: Recogn. 3:Cued Recall 4: Cued Recogn.	1	4	2	2	2	2	3	1	1	1	3	4	1
	1: Cognometrics 2: Locimetrics 3: Drawmetrics	-	2	1	1	1	2	2	1	3	3	1	1	3
	1: User chosen 2: User selected 3: System Gener	1 or 3	2	2	2	3	2 → 3	2	2	1	1	3 → 1	2	1
	Memory Burden	Length of min, 8	Mnemonic, for each step 1 elem.	Mult. sel. images	Mult. images of the same colors	Mult. gen. images	4 chosen images	Mult. elem. In a single image	4 connected loc. on a grid	Personal drawing	Drawing lines betw. 9 dots	Key-pairs of two for each inkblot	Mnemonic, for each step 4 pict.	Drawing limited to 8 stroke direc.
	Memory training and interference													
Complexity	Multiple steps with or without predefined order	Single step order	Multi step order	Multi step	Multi step	Multi step	Single step order	Multi step order	Single step order	Single step order	Single step order	Single step order	Multi step order	Single step order
	Password Space (complexity)	94^N	60^N	9^N			10000		10000		9!	52^N	3024	± 10000
Technical	Input of password (Touch/Click, keypad/keyboard)	Keys	Both	Click	Click	Click	Keys	Click + drag drop	Keys	Draw	Draw	Keys	Click	Draw
	Password Storage	Text	Digit			Text			Digit	Digit	Digit	Text		Text
	Multi platform	+/-	++	++	+/-	+/-	+/-	+/-	++		Mob.	++	+/-	
Security	Dictionary attack	- -		++	++	++	++	-	+	-	-	++	+	-
	Brute force attack	+/-					++				+			
	Shoulder surfing	- -	++	-	++	-	+	-	+	+	-	++	+	+
	Phishing attack	- -	+	+	+	+	-	- -	+	- -	- -	++	+	+
	Man in the middle attack	- -	++	+	-	-	++		++	-	-	- -	+	+
	Guessing attack	-	++	-	++	++	+	-	-	+	-	++	-	-
Graphical	Distinction colors, shapes /images	-	+	++	+	++	++	++	-	- -	+	+	+	-
	Combination of graphics	- -	++	- -	+	- -	-	+	- -	- -	- -	+	- -	- -

Table 1: Simplified Classification Matrix: - - is low score, ++ is high score

The last aspect of Memory is training. How many (training) trials does a user have to complete in order to successfully input the password within a reasonable time [11]. This variable is included in the classification matrix, but an actual comparison has been left out due to the lack of data about this variable for both *PicassoPass* and the other graphical password schemes.

Complexity

The second category is Complexity. Two variables of Complexity are identified: the actual, mathematical complexity [18] and the order of password input. The former is straightforward, although there are differences in the notation of the complexity.

Password input could be based on a predefined order or based on random input order [14]. When the scheme is order based, the user has to repeat the steps during input exactly as when the password was created. The more steps are required, the higher the chance that the user makes a mistake [3]. Other schemes are giving a user the possibility to input the password in any order, which can confuse the user due to forgotten steps or actions.

There is also a difference between inputting the password within a single environment, like a single window or input field, or within multiple environments like multiple windows or steps. Some of the schemes are combining single step input with multiple step input [18].

Technical

The Technical category is the third category of the classification matrix. The purpose of this category is to indicate how users have to enter their password, by means of keyboard, touch, point & click or by using gestures [3, 10]. Keyboard entry could be used in combination with displaying (alpha)numeric values on top of the graphical passwords that have to be inputted into a text field [4].

Another technical aspect of the schemes is how the password is stored. When it is stored as plain text it is less secure than a hashed or encrypted password [3]. Sometimes a `portfolio` of images is stored for each user [11], taking up a lot of disk space [10]. For only a few investigated schemes the (secure) storage of the password was described, so our comparison on this aspect is incomplete.

The last aspect of the Technical category is whether the scheme is suitable for various platforms, like mobile, ATM, computer, tablet and if this aspect was taken into account from the start [1, 3, 8].

Security

The next category is Security, which is reflected in how resistant a scheme is against different types of attacks. A dictionary attack is related to the uniqueness of a password and if applicable, how many hotspots are present within a graphical password scheme [18]. A hotspot is a popular spot within an image for many users, making it very likely that an average user has also chosen this spot. First trying to abuse these spots can limit the amount of work for attackers. A user-specific image collection (so no or as less as possible common data between users) narrows down the possibility of a dictionary attack [11].

When a scheme is resistant to brute force attacks [13] it is impossible to try all combinations, due to, for example, a time-out or variation within the scheme during login.

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 [3]. This can also be achieved with recording devices like camera's [3], but also by using keyloggers, screenscrapers (to see what is happening on screen) and mouseloggers [18, 12].

A technique to counter shoulder surfing is the use of decoys [8] so malicious users are confused or cannot detect the correct answer unless they capture multiple trials of the login sequence.

A fishing (also known as phishing) attack stands or falls on how well users can describe their passwords [3, 14]. Some schemes are using randomized graphics which are highly recognizable for users while they are very difficult to describe due to not having any resemblance with everyday objects.

Another attack is the man-in-the-middle attack which is based on capturing the data transfer between user and the validating system [3]. Sometimes the actual password can be captured because it is sent as plain text. Sending it in an encrypted format is not always more secure, an attacker could hijack an encrypted password and use this to login when there is not a validation of when the password is inputted or from which device or location it was submitted. The encrypted password is likely to be the same every time, unless a time-based or one time valid token or randomized data is being used [11].

The last attack being defined within the Security category is guessing attack, where personal information, like gender or individual preferences, is used to guess the password. An example of information that can be used for a guessing attack is that people prefer faces of the opposite gender [3, 14].

Graphical

The final category is Graphical, with two variables: distinction and combination. The better the distinction is between colors, shapes and images, the fewer mistakes users make during input [1, 8], however it also increases the risk for successful dictionary and shoulder surfing attacks. Note that a good distinction between shapes also makes it possible for colorblind people to use the password scheme [3].

Combining graphical elements increases the strength of passwords and the theoretical password space, but is being used in only a very few graphical password schemes. Typically the used images or graphical elements that are being displayed are positioned within a grid [3, 14] instead of being combined. This aspect is discussed in detail in the next chapter.

DYNAMIC COMBINATION OF GRAPHICAL ELEMENTS

Only a few graphical password schemes are combining graphical elements. 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 is Passfaces [3, 10, 15, 19, 21]. Passfaces only 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.

An example of a graphical password scheme that uses this technique is Picture Password [10, 15]. Users can select two images from a grid, which acts similar to the shift key on a keyboard and forms a unique combination. However, Picture Password increases it's password space mostly by displaying 30 different graphical elements. Fitts' Law from 1954 then comes in: the time to point to a target depends on the distance (or total size) and size of the target. So, when the distance (or total size) becomes larger and the targets smaller, the performance becomes slower [20].

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, she/he 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 complicated things more for shoulder surfers, especially if the combination of layers is different every time (dynamic).

PICASSOPASS

The aforementioned classification matrix and the resulting observations regarding dynamically combining graphical elements, served as inspiration for a novel scheme. This scheme, called *PicassoPass*, scores very high on a particular variable which was underrepresented in existing systems: combining graphics. *PicassoPass* is a challenge-response based graphical password system. It dynamically combines graphical elements in different layers, which hasn't been described previously.

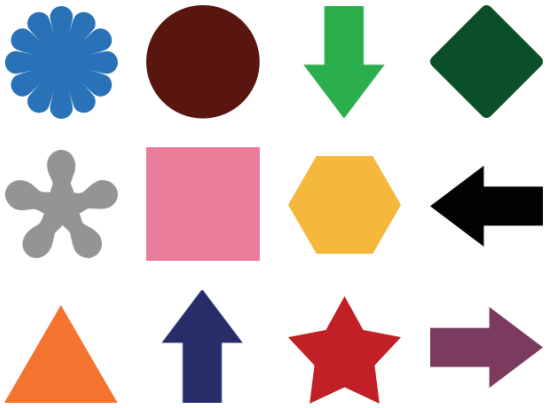

Figure 1: Two layers (shape and color) in one image

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.

Graphical

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 and 3.

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. With every login the elements are randomly combined. 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 2). It would require multiple captures of the login process to rule out all potential reasons.

For every grid / step, the user has chosen what selector is used, like the shape, character, color or the position of the cell. The user is going through each grid one by one until she/he 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.

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.

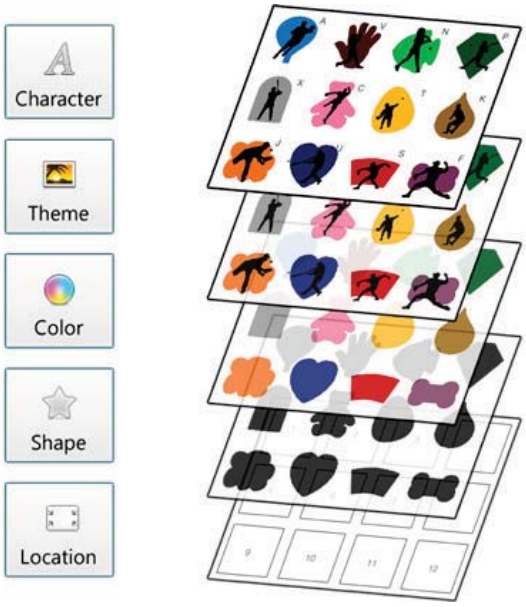

Figure 2: Different Layers of PicassoPass

Technical

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

ATMs with touchscreens could also profit from *PicassoPass*, since due to the layering and random combination of elements, capture attacks will not work unless the target has been recording multiple times with drawing cash during the period the ATM was altered. When ATMs do not have a touchscreen, the amount of cells could be limited to nine so the position of cells corresponds with the actual keyboard layout of the keypad of the ATM. Web based solutions could also use *PicassoPass*, since point & click will also work with the grids and can be scaled up to be used on screens with larger resolutions.

Memory

PicassoPass uses the combination of graphical elements for a mnemonic approach [11]: a story assists the user in the recognition of graphical elements (cued recognition).

A positive effect of a story approach 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 [22], they will be easier to remember [20]. This especially applies to semantically meaningful content like concrete images or real-world scenes (as described by Norman in 1988) [20], which are easier to remember than abstract images.

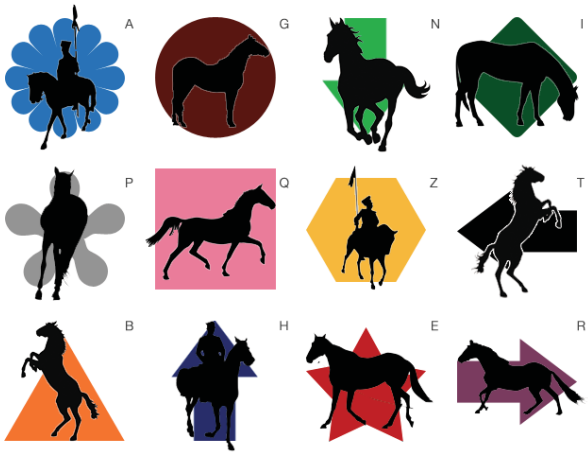

Figure 3: The final result of dynamically combined layers

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 [19, 20]. At the same time, there is a preference for images that are symmetric so memory load can be reduced [13, 16].

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`.

This story-based approach of *PicassoPass* with clear and distinct colors, shapes and images, gives it a significant advantage for memory burden and reducing mistakes.

Due to the mnemonic and graphical approach, users that are illiterate can still login. The layering is also beneficial for color-blind users that have problems distinguishing colors: they can use the other elements like position, shapes, themes and characters.

When the user has forgotten the password, a new one can be requested by entering their username and email address. An email with an unique URL with limited lifespan (1 hour maximum) will be sent to the user, after the username and email address are validated against the list of registered users. When the user clicked the one-time valid URL, the site requests to enter the same username and email address to verify the user. If the verification is successful, the user can create a new password.

Security study: comparison of shoulder surfing attack of PicassoPass with current password schemes on a tablet device

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.

Our null hypothesis of the aforementioned setup is: H0: “There is no difference between the three password techniques when it comes to shoulder surfing attacks.”

In total there were 57 participants (numeric: 18, gesture: 17, *PicassoPass*: 22). Table 1 shows the survey results for the number of successful and unsuccessful participants in guessing the passwords for the different password methods.

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 both of the variables are nominal, the statistical test needed to test the hypothesis is chi-square [7]. Thus, the value of chi-square was 40,94 which was significant at the .1% level with 2 degrees of freedom. 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, when it comes to resistance to shoulder surfing attacks.

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 2). This confirms the potential of *PicassoPass* to protect against shoulder surfing attacks.

Figure 4: Stills of the three different videos

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

Table 2: Number of successful and unsuccessful participants in guessing the passwords for the three password methods

FUTURE RESEARCH

Although these promising first results could be an indication that *PicassoPass* has potential to be an adequate graphical password system, a more complete investigation is needed.

Future studies on the other main categories in the proposed classification framework should confirm this, in particular regarding the expected performance on memory burden and recall. In this section we elaborate three directions we are interested in exploring in the future.

Memory burden

PicassoPass is expected to perform especially well on memory burden (due to its story based approach with clear and distinct colors, shapes and images) and on shoulder surfing resistance. The latter has been tested and confirmed. Future studies should investigate to what extent it enables users to remember their password and clarify issues related to training and interference (for example if using multiple password could lead to password interference).

Usability testing

In this paper we presented a study based on finger-based interaction on a tablet device. Yet we envision PicassoPass to be generically used in all sorts of devices. ATM machines also imply touch-based interaction but what about desktop computers or smart TVs? On such devices mice, keyboards and remote controls are the primary means of interaction. We are interested in investigating how well does PicassoPass performs in terms of efficiency but also satisfaction from the user's point of view.

User Customization

The version we present in this paper has a set of icons showing sports (figure 2) and horses (figure 3). Nevertheless, this set of icons could potentially be of any given theme. One could imagine being able to customize the icon set based on a favorite movie or TV show or video-game. That could of course work for a specific set of devices but at the same time raises new, interesting questions of technical nature and its generic applicability. The similarities of the icon set could also lead to interference of remembering the password due to too many similarities and thus making it harder for the user to correctly input their password.

Security threats

Although shoulder surfing resistance is confirmed in tests, repeatedly shoulder surfing on the same user could possibly result in a successful guess of the password. Other security threats are also noteworthy to investigate, especially how well *PicassoPass* stands against dictionary and brute force attacks.

CONCLUSION

A systematic review of 35 graphical password schemes yielded a new classification which we propose as a novel way of looking at password schemes that would help designers of such schemes position their work. This classification allowed us to identify that combining graphical elements for a graphical password scheme is not often utilized, let alone a dynamic combination of layers which increases password space.

Based on this discovery, we developed a new graphical password scheme called *PicassoPass*. *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. Its resistance to shoulder surfing attacks has been tested and confirmed. These results proved that it has potential to be investigated further.

REFERENCES

1. A. D. Angeli, L. Coventry, G. Johnson, and K. Renaud. Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 2005.
2. K. Bicakci, M. Yuceel, B. Erdeniz, H. Gurbaslar, and N. Atalay. Graphical passwords as browser extension: implementation and usability study. Technical report, 2009.
3. R. Biddle, S. Chiasson, and P. van Oorschot. Graphical passwords: learning from the first twelve years. Technical report, 2011.
4. S. Brostoff, P. Inglesant, and M. Sasse. Evaluating the usability and security of a graphical one- time pin system. In Proceedings of the 24th BCS Conference on Human Computer Interaction - HCI2010, 2010.
5. K. Chalkias, A. Alexiadis, and G. Stephanides. A multi-grid graphical password scheme, 2008.
6. S. Chiasson and et al. A second look at the usability of click-based graphical passwords. In ACM SOUPS, pages 1-12. Press, 2007.
7. S. Chiasson, P. C. V. Oorschot, and R. Biddle. Graphical password authentication using cued click-points. In 12 th European Symposium On Research In Computer Security (ESORICS), 2007. Springer-Verlag, 2007.
8. A. De Angeli, L. Coventry, G. Johnson, and K. Renaud. Evaluating the usability and security of a graphical one-

time pin system. In International Journal of Human-Computer Studies, volume 63, 2005.

9. A. E. Dirik, N. Memon, and J. camille Birget. Modeling user choice in the passpoints graphical password scheme. In In SOUPS 07: Proceedings of the 3rd symposium on Usable privacy and security, pages 20-28. ACM, 2007.
10. S. Gkarai and A. Economides. Comparing the proof by knowledge authentication techniques. In International Journal of Computer Science and Security, volume 4, pages 237-255, 2010.
11. R. A. Khot, K. Srinathan, and P. Kumaraguru. Marasim: a novel jigsaw based authentication scheme using tagging. In Proceedings of the 2011 annual conference on Human factors in computing systems, CHI '11, pages 2605-2614, New York, NY, USA, 2011. ACM.
12. M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd. Reducing shoulder-surfing by using gaze-based password entry, 2007.
13. D. Nali and J. Thorpe. Analyzing user choice in graphical passwords. Technical report, 2004.
14. X. Suo, U. Direction, Y. Zhu, X. Suo, and X. Suo. A design and analysis of graphical password, 2006.
15. H. Tao. Pass-go, a new graphical password scheme, 2006.
16. J. Thorpe and P. van Oorschot. Graphical dictionaries and the memorable space of graphical passwords. In Proceedings of the 13th USENIX Security Symposium, 2004.
17. J. Thorpe and P. van Oorschot. Towards secure design choices for implementing graphical passwords, 2004.
18. J. Thorpe and P. van Oorschot. Human-seeded attacks and exploiting hot-spots in graphical passwords. In Proceedings of the 16th USENIX Security Symposium, 2007.
19. S. Wiedenbeck, J. Waters, A. Brodskiy, and N. Memon. Authentication using graphical passwords: Effects of tolerance and image choice. In In First Symposium on Usable Privacy and Security (SOUPS 2005, pages 1-12. ACM Press, 2005.
20. S. Wiedenbeck, J. Waters, J. camille Birget, A. Brodskiy, and N. Memon. Passpoints: Design and longitudinal evaluation of a graphical password system, 2005.
21. S. Wiedenbeck, J. Waters, L. Sobrado, and J. Birgit. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the advanced visual interfaces symposium, 2006.
22. L. Zin, Q. Sun, and D. Giusto. An association-based graphical password design resistant to shoulder-surfing attack. In Proceedings of the IEEE international conference on multimedia and expo, pages 245-248, 2005.

APPENDIX

A. List of Evaluated Graphical Password Schemes

The following password schemes were evaluated using the comparison matrix, in random order. Since *PicassoPass* is based on the results of the comparison matrix, and textual passwords not being a graphical password scheme, the total number of schemes is 35.

- Awase-E
- Passfaces
- ColorLogin|
- Déjà Vu
- GPEX
- GPI and GPIS
- MARASIM
- Picture Password
- Use Your Illusion
- V-GO
- VisKey
- VIP
- DAS
- GrIDsure
- PassDoodle
- Pass-Go
- PassShapes
- PatternLock
- RAF
- CCP and PCCP
- ImageShield
- Inkblots
- Jiminy
- Loci-based
- PassPoints and PassPoints blur
- Story Scheme
- ColorPIN
- Color-rings
- Gaze based
- Movable frame
- S3PAS
- ShieldPIN
- SlotPIN
- CuePIN
- Convex Hul