International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.15-22
http://dx.doi.org/10.14257/ijsia.2015.9.8.02

Tangramrine: A Novel Graphical Recognition and Cued-recall based Password System

Steven Altamirano[a], Jesús Zanelli[a], Juan M. Gutiérrez Cárdenas[a,b] and Daniela Bringas[a]

[a]*Faculty of Information Systems, Universidad San Ignacio de Loyola. Lima, Perú*
[b]*Faculty of Engineering, Universidad del Pacífico. Lima, Perú*
{steven.altamirano.guevara,jzanellidrago}@gmail.com,
jm.gutierrezc@up.edu.pe,danibrin94@hotmail.com

Abstract

Graphical passwords are an authentication user model that consists of the recall of pictures or graphics signs to gain access to a system. They have been proved to be a secure and reliable alternative to textual passwords; by giving a more robust schema against brute force and shoulder-surfing attacks. In this research paper we present an alternative to a graphical password based on a modification of the Tangram game. We believe our proposal accomplishes the features of being an easy recognition-based system password giving the user enough security against common threats such as brute force attacks by dictionary means or OCR types, as well as shoulder-surfing attacks.

Keywords: *Graphical Password, Authentication, Usability, Security, Memory scheme*

1. Introduction

Password authentication based on textual schemas has been a common attack focus by diverse means and techniques. The most typical ones relied on the use of dictionaries attacks, based on combinations of user and passwords lists; until the system is broken via a brute force algorithm. Another common attack is known as shoulder-surfing; in this scenario the user is vulnerable by the presence of a third-party individual who observes or sneaks during the typing of the password. In a way to countermeasure some of these offensive threats, *e.g.* brute force related; programmers have developed some ideas such as the use of OCR - optical character recognition- captchas, such that the system would recognize if the user attempting to gain admission is a human being or a robot making a brute force attack. In other schemas the user should enter the result of simple arithmetic or general questions in an attempt to enforce the security of one of these systems [8]. Nevertheless these attempts have proven to be weak against more sophisticated attacks, using an OCR algorithm that could recognize the issued captcha, making these systems susceptible again to brute force attacks.

In this scenario the need to outperform the classic textual passwords has brought some alternatives, such as the use of randomly generated passwords. These schemas seem a fairly secure alternative, but the security gained is diminished in terms of the system usability and password memorability.

Graphical passwords were developed as an alternative to the classic textual ones, in a way that the security is enforced, i.e. diminishing brute force attacks; and increasing the recall of the chosen password by a user. Even though these schemas are also prone to attacks, they are somewhat more reliable than textual passwords against threats such as those we described at the beginning of this section.

In this research work we develop the idea of a graphical password based on a modification of the Tangram game; the tests of usability and password memorability among a

ISSN: 1738-9976 IJSIA

group of users proof that this schema is reliable without jeopardizing the system usability. In short, our research work is based on the assumption that "pictures are easier to remember and more secure than words" [9].

We have divided this paper into the following sections: In Section 2 we describe some classic and state-of-the-art graphical passwords. Section 3 describes our proposal in detail. Section 4 deals with the test of our developed software within a group of users; and finally we give some recommendations and conclusions of the current work.

2. Types of Graphical Passwords

According to [1, 10, 13] these schemas are usually divided based on the memory task they involve in remembering and entering the password, and their division into the following categories:

Recall-based Systems: They are also known as drawmetric [5]. In this type of schema the user is prompted to draw its password into a canvas on a PDA-like device. As it is supposed a common attack is a shoulder-surfing attack, mainly because the user has to draw its password into a section of the screen. The weakness of these systems relies also in the characterization of some users to sketch text on the drawing part; also it is vulnerable to phishing attacks by mimicking the structure and canvas of the original login page. An example of a recall-based system is the technique proposed by Jermyn et al. [9] and named Draw-a-Secret. In this proposal the user authentication is obtained by re-drawing his password on an empty canvas: see Figure 1a. This system was made for using the capabilities of, at that time, upcoming PDA technologies.

Recognition-based Systems: Also referred to as cognometric [1, 5], this system is based on the brain's ability to recognize or memorize seen images, which at the end will correspond to their password set. The authentication procedure consists of the user being able to recall the chosen images, identifying them from a set that contains decoys or false images. Among its inner strengths are: High level of memorability, the usability is not only biased towards those people technologically educated, and a fair amount of security [12]. An example of this type of authentication is the technique known as Passfaces [11]; in this scenario the user is presented with a set of images that depict the faces of a set of women and men from different races and ages. The user then chooses a set of images for authentication purposes: see Figure 1b. A probable attack on this system was devised by Davis and Reiter [4]; in this paper the authors proved that the choice of a particular face is determined by the gender, race and even how attractive the person that is appearing on the canvas is. This could lead to a bias for picking some elements over another, in this way leaving room for a sort of "guessing" attack; or that the attacker could determine the password of one user considering the points mentioned before.

Figure 1. Draw-a-Secret schemata; here a user will draw a figure on an empty canvas, the image is then transformed into a grid resolution and then to a bit representation. This system is aware of changes of the pen stroke, or when the input device is not touching the screen, which is a particular inner

characteristic of all PDA based systems. Figure 1b PassFaces, in this system the user is presented with a set of faces or images, which he could select as its chosen password. For authentication purposes the user should select those images that correspond to its password; usually the figures are displayed randomly shuffled at this stage. Figure 1c Passpoints [15], in this schema the user is prompted to choose specific points onto a selected image; this points will correspond to the password that in the authentication phase the user should select in the correct order. There exist other modifications and improvements to this approach, for example, the Pass-Map approach [14].

Cued recall-based Systems: This technique has its roots in the paper published by Blonder [2]; in this schema the user is prompted to select a number of points within an image, the selected points will correspond to the selected password. In the authentication phase the user should recall the sequence of points selected before. Some common attacks to this schemata are shoulder-surfing, the possibility of guessing which points were selected because some sections in the selected image are more prone to be chosen than others. Also by analyzing some portions of the image, an attacker could devise probable selected points by comparing the brightness, hue, saturation and other characteristics of different sections in the user's chosen figure [3, 6, 7]. An example of this schema can be observed in Figure 1c.

3. TAMGRAMRINE Proposal

Our proposal has two separate parts: the memorizing part, in which a user selects a particular password; and the authentication part, in which the user is prompted to enter the memorized password in an attempt to gain access to a system. For the authentication part we decided to use the facial images of a certain number of fictional characters from two well-known cartoon comedy shows: The Simpsons© and Futurama© (Images copyright of Fox Entertainment Group). A first thought about choosing those mainstream shows was that the set of images was going to be easily recognizable by the users performing the tests. It is worth mentioning that the used images were only for research purposes.

3.1 Memorization Phase

In this part we will describe how a user could chose a particular password based on our proposal. First of all, the user is prompted to choose between three or six images of the characters from the aforementioned shows. Each of these images has a background colour and they are enclosed within a specific geometrical form that acts as a frame, see Figure 2.

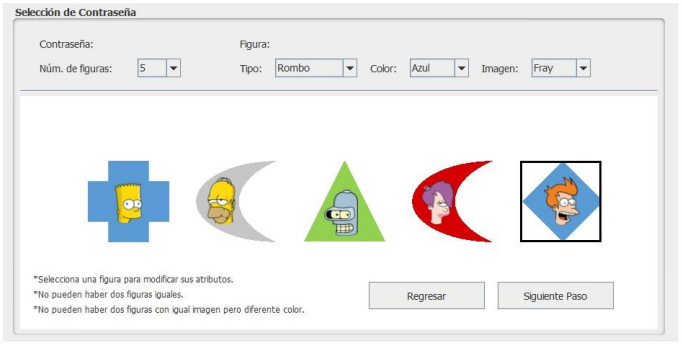


Figure 2. The user can choose between a different set of objects that will contain the desired group of images to be recalled in the authentication phase.

In the next step the user is presented with the figures, but without a background color; this was made in an attempt to prevent a shoulder-surfing attack; because in the authentication phase the user should also remember the background color chosen for each of the figures. The selected figures appear also with a set of points over the borders. These sets of points will act like magnetic points that will allow to join one figure with another, in a sort of the classic Tangram game: see Figure 3.

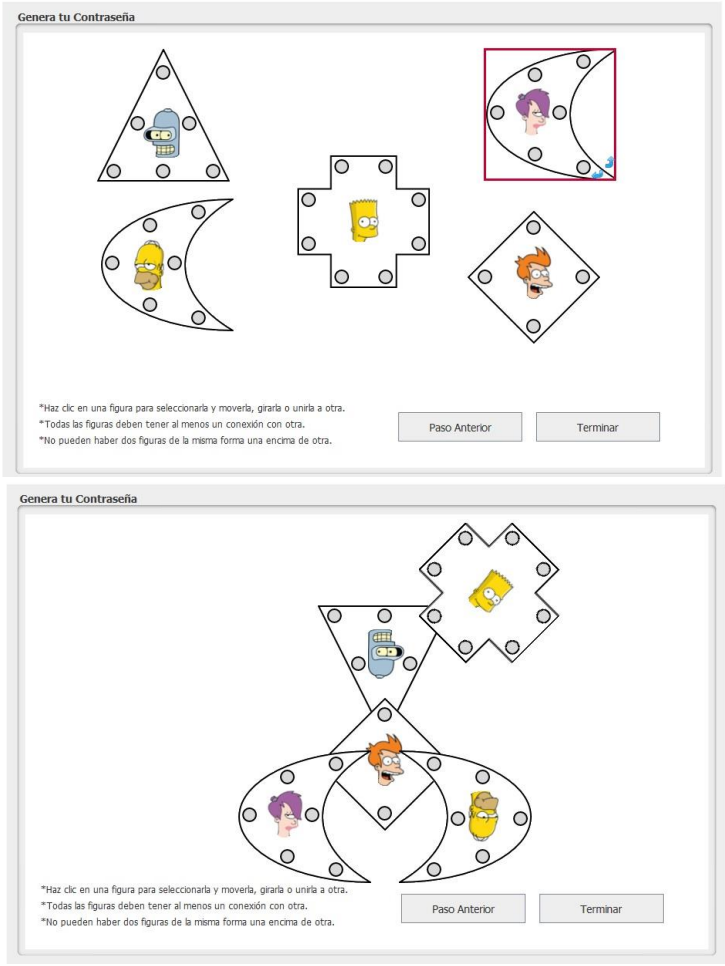


Figure 3. The images without a background colour appear with a set of connection points (a). The user is free to rotate each figure by 45 degrees. In the end, the images are reunited by joining the "magnetic" points forming a final figure. This last figure corresponds to the user password selected by the user (b).

As we can see the user should memorize the inside figures and the pictures with the color frames that hold them. After that, he arranges them by forming a figure that will be his chosen password.

3.2 Authentication Phase

When the user wants to authenticate into the system, after entering his name or email as a user; he will be introduced to a set of randomly generated figures, within them there are the figures that he chose first during the previous phase, see Figure 4.

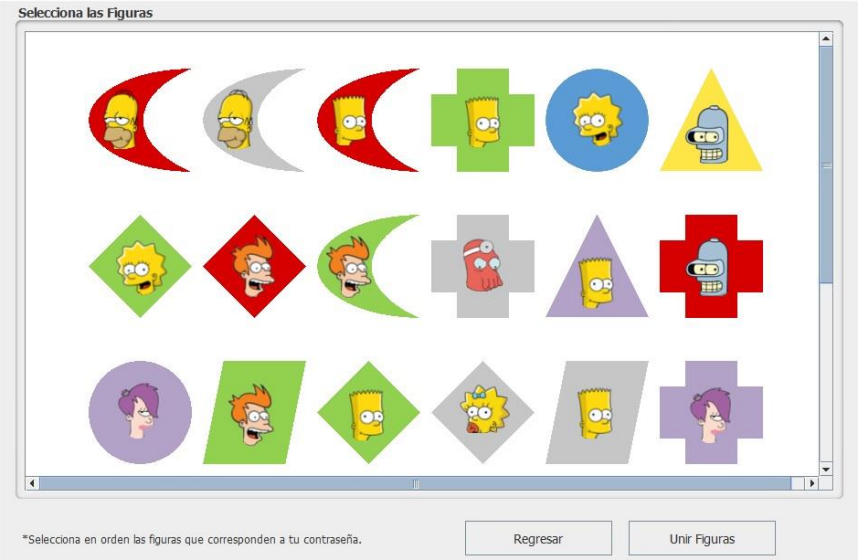


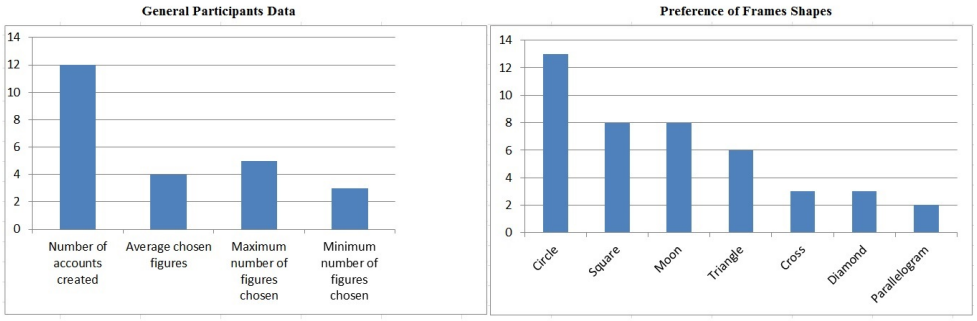
Figure 4. Random figures generated in which the previously selected images are embedded. The user should select the chosen figures and with them try to build the final figure, which will correspond to his password. In case that the user selects a wrong set of figures, he can proceed to the building of the final password; the reason for doing this was for not giving cues of which passwords were correct.

After the user has chosen the correct set of figures, he will be prompted to try to rebuild the connected final figure that corresponds to his password. In this stage one can also put a limit on the login attempts performed by a potential user, in a way to strengthen the authentication part of our proposal.

4. Results

Twelve students declared their availability to perform the testing part of our proposal, of those students only eight assisted in all the reunions established. The students were chosen randomly and most of them were following their first and second year in our faculty of Information Systems. We will begin by showing data related to the preferences of the students in the part of choosing the figures and building their password; also the rate of success and failures measured during the authentication phase.

In the first part, as we mentioned before, the user is prompted to select between a set of figures, and with them try to from a figure that at the end will be their chosen password. In Figure 5 we show the data about which main figures, shapes of the frames, and background colour were chosen among all of our participants.



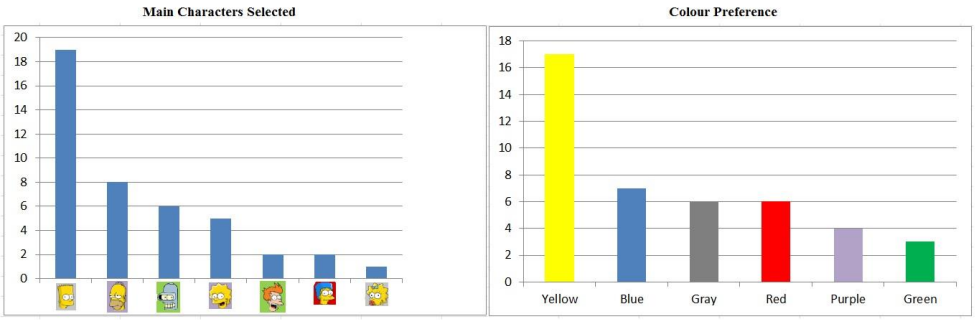


Figure 5. We depict information about how many participants agreed to be part of our tests. Information also related to main characters chosen, selected frames that enclose the main figure, and colours of them are showed.

To gather information about the memorability of our system we divide the authentication process in two steps: The first one is related to the selection of the objects that in the next step will be joined to form a shape; and second the ordering of the figures. There were considered to be three sessions:

Session 1: The user was prompted to familiarize themselves with our system. After the student felt comfortable he proceeded to choose the figures and form the figure that would correspond to his password. After testing his password, he had to wait approximately ten minutes, performing other distractive activity as suggested in [10], to see if he could remember it.

Session 2: This second reunion was made after a period of one week; the users were asked to try to gain access to the system by entering the password they made in the first session.

Session 3: Similar to session 2, the user was prompted to enter his password, and after that, a questionnaire was applied to gather information about general aspects of our proposal. This session was made after a gap of three weeks. The results are shown in Table 1:

Table 1. We present a summary of the memorability results derived from our proposal. The selection attempt consisted in choosing the set of figures while the ordering attempt refers to put the figures in order. We count each attempt of performing these actions, and dismiss any other login attempt during an allocated session, if the user managed to authenticate into our system previously on that session.

Student	Selection attempts	Correct	Wrong	P. Selection
1	5	4	1	80.00%
2	4	3	1	75.00%
3	5	2	3	40.00%
4	6	6	0	100.00%
5	4	4	0	100.00%
6	6	6	0	100.00%
7	6	5	1	83.33%
8	4	4	0	100.00%
			Average	84.79%

Student	Ordering attempts	Correct	Wrong	P. Ordering
1	5	4	1	80.00%

2	4	3	1	75.00%
3	5	2	3	40.00%
4	6	4	2	66.67%
5	4	4	0	100.00%
6	6	4	2	66.67%
7	6	4	2	66.67%
8	4	4	0	100.00%
			Average	74.38%

As we can observe from Table 1 the average results for the memorability part of selection and forming the passwords are well above the 70 percent of correct attempts; at this point, and given the gap between testing sessions, we can hypothesize that our proposal has an adequate level of usability and memorability of the passwords chosen by the users.

4.1 Authentication Phase

We will analyze the number of attempts that a probable attacker will have to perform, when using a brute-force technique, for the first section of trying to guess the figures:

Let's suppose that a user in average selects *N* number of figures, according to our schema were four in average. He also has the chance to select *C* colours, mixed with *S* shapes and *I* images that could be put within; so according to this schema an attacker would have to test:

$$(C*S*I)^N,$$

combinations if he applies a brute force attack; which is approximately 2.04x10E trials. As we can see it is fairly a large amount of trials that a potential attacker would have to do. Of course, our proposal is also susceptible to shoulder-surfing attacks, but the inclusion of non-coloured figures during the last part of the authentication part can enforce our schema.

4.2 Questionnaire

At the end of the trials a questionnaire was submitted to the students, so they could be free to transmit their opinions about the chosen schemata. The questions were the following:

1. Was it easy to build your password? Do you have any suggestion for this part?
2. Do you find the usability of the program adequate? Would you suggest any changes?
3. Do you think that our chosen set of figures made them easy to remember? Would you suggest to use another set of figures?
4. What do you think would be the main difficulty that a user without too much technological knowledge would face, if he wants to use our proposal?
5. State any other suggestion that was not highlighted in the other points.

We will present now the summarized results for each of the questions taken in the questionnaire:

Q1: Six users found the password building part to be an easy task. Two users complained, but not about the building part per se, but about memorability issues to recall the password formed.

Q2: Six users again found our proposal to be a good one in terms of usability; two students stated that there were too many steps for the authentication process.

Q3: About our proposed set of figures, 7 users found that the chosen set of pictures was easy to remember due to the popularity of the given images. One user suggested to choose figures more appealing and that could catch the attention of the user; maybe in a way to help to memorize the sequence of images better.

Q4: About the usability of our system for people that are illiterate in the use of technologies, there were not really any suggestions about this specific part. Instead 5 users suggested that the most difficult part would be to remember the ordering of the images to form the final password; even though they managed to do it quite well according to the results in table 1. One user made a comment that in general people are used to textual passwords schemas.

Q5: In the part of stating any other suggestions or comments, two students proposed to use other types of figures that eventually could be memorable for a larger audience. Two other students proposed to use coloured letters as the figures to be chosen to form the password. About this later suggestion, we believe that by using that proposal, the password formed would be more susceptible to be memorized by a sniffer that performs a shoulder-surfing attack on our system.

5. Conclusions and Future Work

We have presented a new graphical password proposal based on a subtle modification of the classic game known as Tangram. The memorability of our proposal and ease of use, according to the data collected, make it suitable for systems that would like to base their identification tasks on using graphical passwords. We plan to continue this approach and to see if this proposal could apply also to mobile devices. We believe that graphical passwords, if used correctly, could prove to be safer than their textual counterparts, without jeopardizing the memorability as occurs in randomly generated passwords

References

[1] R. Biddle, S. Chiasson and V. Oorschot, "P.C.: Graphical passwords: Learning from the first twelve years", ACM Computing Surveys, vol. 44, no. 4, (**2012**), pp. 19:1–19:41.
[2] G. E. Blonder, "Graphical Passwords", United States Patent, vol. 5, (**1996**), pp. 559, 961.
[3] S. Chiasson, "User interface design affects security: patterns in click-based graphical passwords", International Journal of Information Security, vol. 8, no. 6, (**2009**), pp. 387-398
[4] D. Davis, F. Monrose and M. K. Reiter, "On User Choice in Graphical Password Schemes", In: 13th USENIX Security Symposium, (**2004**).
[5] A. De Angeli, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems", International Journal of Human-Computer Studies, vol. 63, nos. 1-2, (**2005**), pp. 128-152.
[6] A. E. Dirik, N. Menon and J. C. Birget, "Modeling user choice in the PassPoints graphical password scheme", In: ACM Symposium on Usable Privacy and Security (SOUPS) (**2007**).
[7] K. Golofit, "Click passwords under investigation", In: European Symposium on Research in Computer Security (ESORICS). LNCS, vol. 4734, (**2007**), pp. 343–358.
[8] J. Gutiérrez-Cárdenas, W. Bardales and L. Orihuela, "Graph Coloring for Enforcing Password Identification against Brute Force Attacks", In: 23rd. International Conference on Computers and Their Applications, ISCA (**2008**).
[9] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, "The design and analysis of graphical passwords", In: 8th USENIX Security Symposium, (**1999**).
[10] H. Kumar, "Graphical Password Authentication Schemes: Current Status and Key Issues", IJCSI (**2013**).
[11] PASSFACES CORPORATION. The science behind Passfaces. White paper. http://www.passfaces.com/enterprise/resources/white_papers.htm. Accessed 16 March 2015
[12] R. Rohit Ashok Khot, "WYSWYE: shoulder surfing defense for recognition based graphical passwords", In: Proceedings of the 24th Australian Computer-Human Interaction Conference. OzCHI '12 (**2012**).
[13] E. Stobert and R. Biddle, "Memory retrieval and graphical passwords", In: ACM Symposium on Usable Privacy and Security (SOUPS) (**2013**).
[14] H. Sun, "PassMap: a map based graphical-password authentication system", In: ACM Symposium on Information, Computer and Communications Security (ASIACCS '12) (**2012**).
[15] S. Wiedenbeck, "PassPoints: Design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, vol. 63, nos. 1-2, (**2005**), pp. 102-127.

