Usability Evaluation Using Eye Tracking for Iconographic Authentication on Mobile Devices

Claudia de Andrade Tambascia, Ewerton Martins Menezes, Robson Eudes Duarte
CPqD Foundation
Campinas – SP, Brazil
{claudiat, emenezes, robsond}@cpqd.com.br

***Abstract*— This article aims to present the results of a usability evaluation for the use of iconographic authentication on mobile devices as a way to improve security aspects in handling information. This way of authentication was defined in a project called Multimodal Biometric and Iconographic Authentication for Mobile Devices. These assessments were carried out with eye tracking support tools as a means of proving the difficulty points and allow the design decision could be made more accurate to the application final purpose.**

Keywords-Usability evaluation; iconographic passwords; eye tracking observation

I. INTRODUCTION

Considering that human brain recognizes and reminds visual information better than textual information [1][2][3][4], the usage of authentication mechanisms that explore the later rather than the former represent a new paradigm for safety and usability issues in the context of mobile devices due to increasing demands for safer and more flexible new ways of authentication.

In this context, the iconographic authentication may be used to totally or partially lock the device, configuring one level of authentication, which can be then integrated to biometric techniques to increase safety to the process.

A system for local iconographic authentication, where the password verification happens within the device, with no external database access has been proposed. Usability and accessibility issues must be addressed considering the multiplicity of user profiles, including those with little or no familiarity to computing interfaces, with disabilities or with low literacy.

This paper will describe the methodology used to evaluate the usability of iconographic passwords on mobile devices, in the context of a Multimodal Biometric and Iconographic Authentication project [5], as well as presenting the results obtained taking into account aspects like ease of use and memorization, time spent for authentication and the strategies for password creation. This research is important to determine the viability and the benefits of iconographic passwords in this usage context.

In the following sections, the concepts of iconography and usability applied to mobile devices, the prototype employed for iconographic passwords creation and usages, the methodology of evaluation, results obtained and final considerations will be presented.

The section two will present graphical authentication concepts used in this project followed by section three that will present related works. The section four will present a prototype develop for iconographic passwords followed by section five with test methodology used. The section six will present the obtained results followed by section seven with some conclusions and future works.

II. GRAPHICAL AUTHENTICATION

Graphical authentication is a type of knowledge-based authentication that has been explored for over twelve years. It can be basically categorized in three groups [6]: (1) the recall-based authentication systems, in which the user is asked to recall and reproduce a secret drawing, (2) the cued-recall systems, where the user has to remember, (3) and target specific locations within an image and the recognition-based systems, which usually demand the users to memorize a group of images.

As a recognition technique, the iconographic authentication demands less cognitive load than recalls techniques and tends to increase the usability, the security and the user performance, besides being specially appealing in the mobile context, where typewritten input is less common than pointing at the screen.

While some recognition-based systems use faces [7], assuming that the brain has got a special ability to recognize them, other systems use abstract images [8], which are stronger from a security point of view, due to their difficulty of describing. Nevertheless, the use of icons brings a better compromise between usability and safety, once it facilitates mnemonic strategies and then consequently the memorization.

The security level offered by such systems depends on many factors, such as the length of the repository available to the user, the password length, the input method, and the icons themselves which must ideally show similar probabilities of choice avoiding dictionary attacks.

III. RELATED WORK

According to Nielsen and Mack [9], problems with usability found on an interface might be related to different aspects such as user difficulty in learning how to use a system; user delay to complete his/her tasks; deception of the user in operations caused by the system and non-attractive interfaces. Often, the use of inadequate language causes intelligibility problems, which combined with the above

 ISBN: 978-1-61208-164-9

aspects, further contribute to user dissatisfaction and interfering with the quality of experience.

We can find in literature studies like the Jun Gong's one [10], which is based on Shneiderman's "Golden Rules of Interface Design" that proposes a generic set of guidelines for mobile devices. In addition, it is possible to find main mobile manufacturers recommendations, but they usually cover specific cases [11][12], which evidences the lack of standards and consensus mobile usability field.

To ensure effective application of iconographic authentication and to fulfill the user expectations, specific usability aspects for mobile environment, such as extremely dynamic context use and limited user attention, must be taken into account. Applications must be capable to start, stop and resume with little or no human effort, and also have to provide multiple feedbacks and be customized under user needs.

The mobile devices present hardware limitations related to screen size, processing power and input methods. These facts draw attention to images and text size definition as well as buttons displayed on the interface, so the error and cognitive effort rates can be reduced, besides prioritize the choice of icons rather than text input.

IV. PROTOTYPE FOR ICONOGRAPHIC PASSWORDS

One of the main goals of the use of iconic passwords in process of authentication is to increase usability, assuming that the password memorization gets easier for the visual inclined users, and to ensure the user will keep this information in mind for a longer time.

To evaluate iconographic aspects of the authentication process, such as, quality of icons, repertory length, password length and amount of icons displayed it was implemented a prototype that runs in an Android emulator. With this prototype it was possible to do tests in a conventional desktop using an eye tracker device and analyze the user visual behavior during password creation and usage.

A repertory of seventy-two icons was considered as it is shown at Fig. 1. Each column was filled with a category of icons, totalizing twelve categories with six icons each. With the intention of reaching a balance between usability and security the order of the columns and the placement of the icons within the columns change at each interaction action.

Figure 1. Icons repertory considered in the prototype.

The categories considered for the icons were fruits, animals, technological devices, and means of transportation, balls, sea elements, musical instruments, scholar material, smiles, banners, body parts and hats.

The selection of such icons in each category was made after an analysis of possible strategies to help memorization of iconic passwords and, consequently, usability increase of iconographic authentication, without loss of mathematical security, as presented in [13].

The first screen of the prototype allowed the user to choose the option of creating or using an iconographic password. It was possible to configure the password length, as shown at Fig. 2.

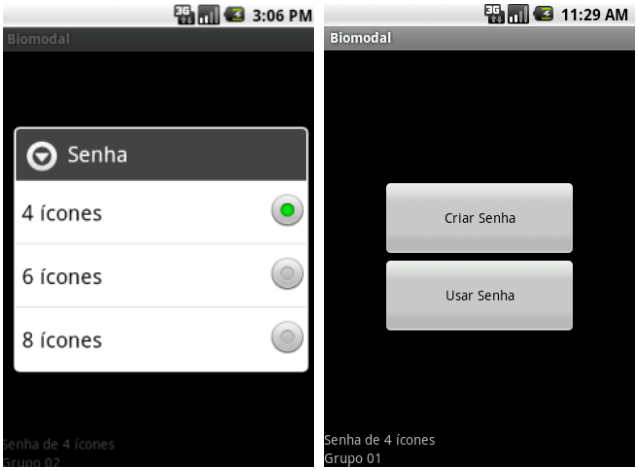

Figure 2. Prototype initial screen.

Passwords were categorized in fixed lengths of four, six and eight icons and tests with five users for each of this category were defined, according to the methodology presented in the following section.

V. TEST METHODOLOGY

A. User selection and tests frequency

The first step for the test realization was to determine the users that would participate on it as well as the frequency of the test sessions.

According to [14], practitioners of usability recommend many different quantities of interviews, for several different reasons. For shipping products, it was recommend six interviews, for the following reasons: i) six one-hour interviews can be conducted in one calendar day; ii) testing six respondents allows you to identify trends. For this project five users were selected for each category of password.

These users were divided into man and woman with under-thirty years old, thirty to forty-five year old and forty-five years old or older, as showed in Fig. 3.

 ISBN: 978-1-61208-164-9

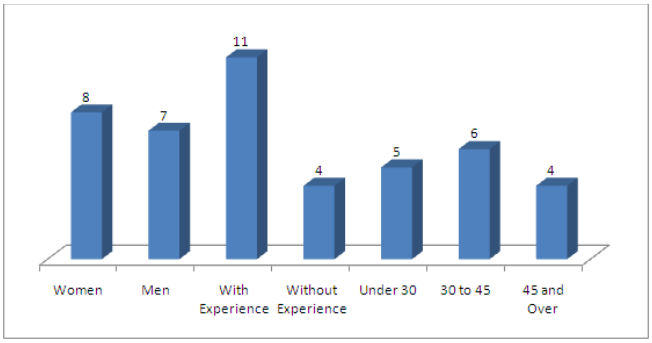

Figure 3. Summary of user profiles (gender, level of experience and age groups).

Such division was necessary once the memorization was to be measured, which implied the need of considering different age groups. It was also taken into account previous experience with mobile devices, for it could influence the usability requirements.

The users were separated into three groups, with five users each to optimize test sessions in a work day. After the four first interactions with the first group, the test sessions with group occurred.

Since one of the main criteria to be evaluated will be the memorization of passwords after a period of time. It was defined that the test would happen during fifteen days according to the schedule presented at Fig. 4.

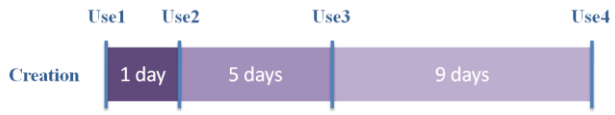

Figure 4. Tests schedule.

The first use was composed by password creation and confirmation. If the user could not be able to remember the password the creation process was restarted. The second use had to be one day after its creation. The third use was planned to happen five days after password creation, encompassing a weekend that could influence password memorization. Finally, the fourth use had to happen nine days after password creation for it was a period considered enough for the password is forgotten in case the memorization strategy failed.

B. *Test configuration*

All the tests were performed in a usability laboratory composed of two rooms: the participant room and the observation room. The eye tracking device employed was Tobii Eye Tracker T60 [15], which consists of a seventeen inches display with cameras and embedded infrared sensors. The iconographic authentication prototype run on this display and the interaction method for selection and browsing was the mouse.

During the test execution users were asked to keep a distance of about sixty centimeters far from the display to enhance eye tracking quality. The screen recording was made together with viewpoints using gaze plots, heat maps, and audio. User's expressions were also important in case the eye tracker might not capture relevant data.

C. *Results tabulation*

After the realization of four tests rounds, the user's performance was grouped according to password length and compared with the time spent during the creation and usage. For passwords with four icons, a concern in the password creation was observed, which lead a better time performance in confirmation task as shown at Fig. 5.

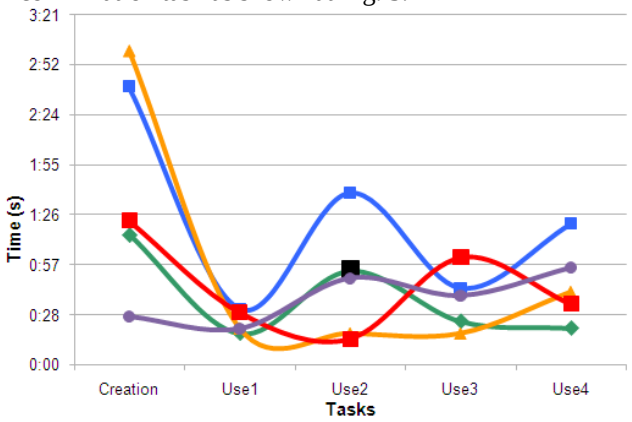

Figure 5. Evolution of users performance for passwords with four icons.

There was only one mistake by one user in his second interaction, identified by a black square in the following graphic shown at Fig. 5. Further interactions happened with no significant changes.

For six icons passwords, the user's behavior presented wider variation and more mistakes after the second interaction, as shown at Fig. 6.

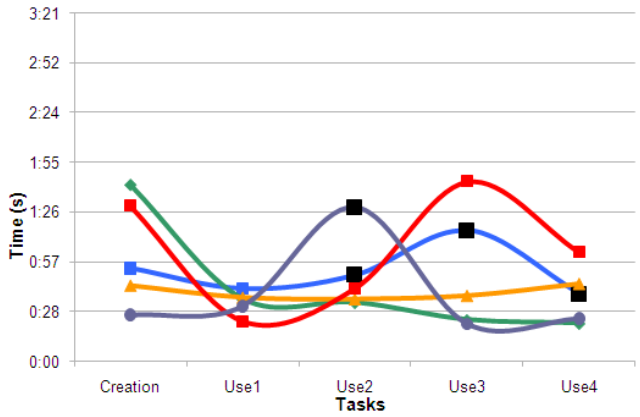

Figure 6. Evolution of users performance for passwords with six icons.

Password creation, compared with four icons password, was faster, which can explain why subsequent interactions lasted longer and had more mistake occurrences.

Finally, for eight icons password, it was possible to observe the best performance in interactions after password creation, except for a user who quickly created the password

 ISBN: 978-1-61208-164-9

and could not remember it in the subsequent interactions (as shown at Fig. 7.

It is important to highlight that the mentioned user made a mistake in the second interaction and last a long at the third one, but after that he would not forget the password anymore, showing satisfactory result in the last interaction

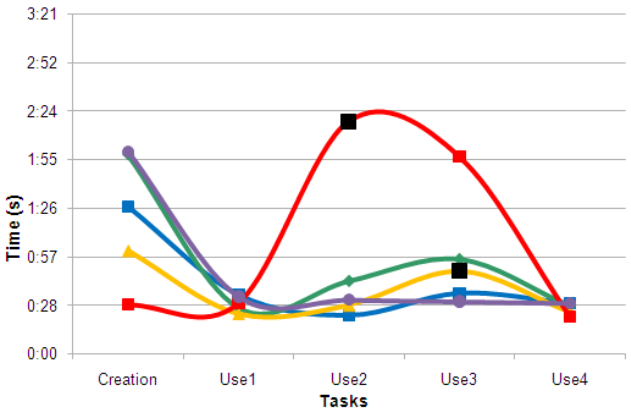

Figure 7. Evolution of users performance for passwords with eight icons.

D. Eye tracking data

Based upon Duchowski's recommendations [16] for experiments involving eye tracking data it was observed the visual behavior of the participants during the iconographic password creation and use processes.

The tests videos were separate into relevant video segments and using the gaze plot resource was possible to compare different ways of exploring visually the grid of icons. Three samples of interaction schemas by the time of password creation were shown in Fig. 8. The circles represent the visual fixation points and its size is proportional to the duration of the look.

(a) (b) (c)

Figure 8. Ways of eye interaction in password creation.

Fig. 8 (a) presents the behavior of a user who analyzes the icons in a chaotic or random way, searching for familiarization among the images for the creation of the password. Fig. 8 (b) presents the behavior of a restrained user that what limits his/her field of view to two categories, aiming at easing password creation. Fig. 8 (c) presents the behavior of a methodical user who observes invariably all icons available on the prototype to make his/her choices.

In all cases of user behavior it was possible to notice a concern in observing icons according to the strategies chosen to ease the memorization process.

E. Memorization strategies

After password creation, the test conductors tried to infer the strategy used to memorize it. At the end of the round of testes the users were briefly interviewed and asked about strategies used and face difficulties.

During the test realization it was observed that iconographic passwords enable a wide universe of possible combinations which favors the use of most varied strategies of memorization and creation of passwords that are stronger and less susceptible to dictionary attack.

The strategies are extremely dependents on the repertory of icons used and the amount of icons to be memorized and a direct relation among the level of difficulty perceived by each user was observed.

Table 1 shows a categorization of strategies used by each participant of the tests.

TABLE I. MEMORIZATION STRATEGIES

Strategies	Users
Peer association	5
Creating history	3
Category elimination	3
Icons with similiar colors	2
Cultural issues	2
Memorization of individual icons	2
Visual affinity with icon	2
None specific	9

Have a fixed or a free password order strongly influences the creations strategies and for this reason it was not announced to the participants that the icons order did not matter on creation process. Even so, many users created and used the password in order, especially in the cases where there were associations of the icons to stories or sentences. Nonetheless, the larger the password was, the less users selected icons in the created order.

VI. RESULTS

Many performance factors such as the execution time, error rates, screen browsing and password memorization in a time interval were evaluated.

In this context, passwords composed by four icons were the ones which presented best use performance, with lower error rates and time average in all interactions. The eight icons passwords were the ones with more occurrences of history creation as a way to improve the memorization and when histories were not created, the elimination of categories was used to reduce the possibilities and to ease the password creation.

It was possible to observe that there is not a direct relation between the quantity of icons in a password and the time necessary for authentication, for users with different

 ISBN: 978-1-61208-164-9

password sizes get very similar performance in authentication. However, the time spent to create passwords may influence directly its memorization, that is, users who spent more time creating the password had less error rates and tended to not forget it.

This fact was ratified by testimonies of the users who have not remembered the password and assigned it to the lack of attention by the time of the password creation. It indicates the need of thinking about strategies which may favor the password memorization.

As one of the premises of the test was that it did not need to be entered in the creation order, many users that had initially created strategies prioritizing the icons order finished by abstracting this strategy as the familiarization to the password increased. It corroborates researches that point as a usability factor the use of passwords by order and disorder, a different paradigm from the one used for traditional passwords.

The choice frequency of the icons to compose the iconographic passwords was another important factor. It was possible to observe a regular distribution of the icons where the most and less chosen categories kept constant, as shown at Figure 9.

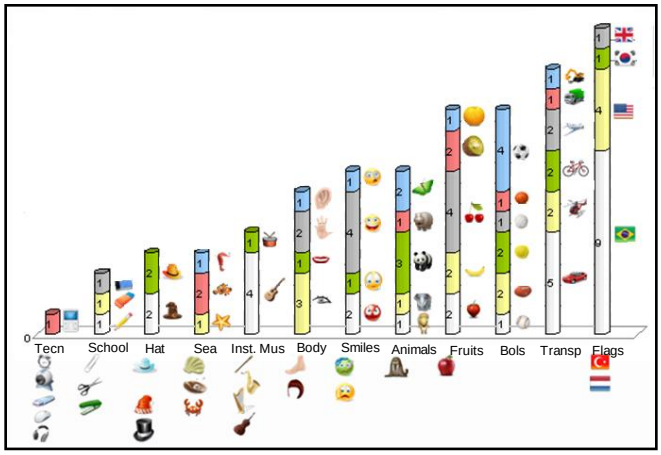

Figure 9. Distribution of icons chosen by the participants.

The user preference for gaudy icons was also observed. The icons under technology devices category, which were the less chosen ones, had grey as predominant color. However, cultural and esthetic aspects had major choice weight. For this reason, icons such as Brazilian banner, soccer ball, red car, and cherry were chosen much more than orders.

The appropriated feedback at the authentication proved to be a key factor to guide the user throughout the process. As observed in the survey the user needs to know how many icons have already been chosen, should be clear the number of screens, if there are more than one, and the current screen. This information must be presented to users in clear and non-blocking way avoiding the slowdown of the authentication process.

At last, it was identified a characteristic named “love at first sight” that consists of a situation in which the user thinks about choosing an icon to compose his/her password, but he/she does not do so. By the time of the authentication, the user then finds him/herself in doubt about chosen and will not know whether it compounds or not the password. This problem may be solved by considering a little training process just after password submission. This training may include, e.g., three authentication simulations before password registration. Alternatively, the system could itself choose the password for the user what, on the other hand, could reduce the usability of the solution.

VII. CONCLUSIONS AND FUTURE WORKS

As the use of icons to make authentication can be considered a new paradigm, it was adopted an initial approach considering six icons passwords to reach an adequate usability level and allowing the use of histories to ease memorization and reducing time spent for creation and use of the passwords.

On the other hand, it is reasonable to claim that as the familiarity of the users to this new paradigm increases, the results of usability tests will be better either. And higher levels of security will also be reached.

At last, in the performed tests it was also observed a preference for some icons instead of others, what may weaken the security of iconographic authentication. But there is a positive feature that reduces this risk which is the possibility of substituting some icons as well as letting to the system the definition of the password.

Considering the security and usability aspects presented in the Sections II and III, some project decisions were established to lead the prototype implementation. In a general way, the users that made the usability tests with four icons did not only have a very good performance but also reported that it was easy to memorize only four icons. As for the six and eight password users, they had very heterogeneous test result and performance.

The security comparison between iconographic and alphanumeric passwords in the evaluated scenarios, it was defined an initial password size of six icons within a repertory of ninety icons. This repertory was split into three screens with thirty icons each (six rows and five columns). The use of bigger repertory of icons impacts significantly in the usability of the solution, resulting in the increasing of the security not proportional to this impact, which makes impossible the use of a bigger repertory. As for the size of the password, it could be bigger, and it would result in an increment of security for the solution. But, as it deals with a paradigm change, it was decided to maintain initially the six icons for iconographic authentication.

The tests performed in the context of this project have presented an analysis, which contributes for the definition of the iconographic authentication solution that will be used for implementation of the functional prototype of project Multimodal Biometric and Iconographic Authentication for Mobile Devices.

Despite the missing standardization among the methods it’s possible to ensure that iconographic password systems meet the usability and security requirements. As a future work it’s necessary to provide a comparison between the

 ISBN: 978-1-61208-164-9

performance of iconographic and alphanumeric paradigms, besides test the proposed solution in real mobile devices with dynamic usage contexts.

ACKNOWLEDGMENT

We express our gratitude to FUNTTEL – Fundo Nacional das Telecomunicações, do Ministério das Comunicações, which funds this research.

REFERENCES

[1] B. Kirkpatrick. "An experimental study of memory". Psychological Review, 1894, 1:602-609.

[2] S. Madigan. "Picture memory". In J. Yuille, editor, "Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio", cap.3, pp.65-89. Lawrence Erlbaum Associates, 1983.

[3] A. Paivio, T. Rogers, and P.C. Smythe. "Why are pictures easier to recall than words?" Psychonomic Science, 1968, 11(4):137-138.

[4] R. Shepard. "Recognition memory for words, sentences, and pictures". Journal of Verbal Learning and Verbal Behavior, 1967, 6: pp. 156-163.

[5] R.P.V. Violato, M.U. Neto, F.O. Simões, I.M.A. Ávila, M.A. Angeloni, T.F. Pereira, E.T. Nakamura, and R.S. Cividanes. "BIOMODAL Project – Multimodal Biometric Authentication and Image-Based Authentication for Mobile Devices". 8th Sumer School for Advanced Studies on Biometrics for Secure Authentication. 2011.

[6] R. Biddle, S. Chiasson, and P.C. Van Oorschot. "Graphical Passwords: Learning from the First Twelve Years", School of Computer Science, Carleton University, 2011.

[7] Passfaces Corporation. The Science Behind Passfaces. Write paper, http://www.realuser.com/enterprise/resources/white_ papers. htm, accessed May 2011.

[8] R. Dhamija and A. Perrig. "Déjà Vu: A user study using imagens for authentication". In 9th USENIX Security Symposium, 2000.

[9] J. Nielsen and R. Mack. "Usability Inspection Methods." New York, John Wiley & Sons, Inc.,1994.

[10] J. Gong and P. Tarasewich. "Guidelines for handheld mobile device interface design". College of Computer and Information Science, Northeastern University, Boston, USA, 2004.

[11] R. Blum, K. Khakzar, and W. Winzerling. "Mobile Design Guidelines in the Context of Retail Sales" Support Fulda University of Applied Sciences. Germany, 2008.

[12] S. Chan, X. Fang, J. Brzezinski, Y. Zhou, X. Shuang, and L. Jean. "Usability For Mobile Commerce Across Multiple Form Factors". Journal of Electronic Commerce Research, vol. 3, no. 3, 2002.

[13] I.M.A. Avila, "Estratégias Mnemônicas para Senhas Icônicas", Abril de 2011.

[14] S. Weiss, "Handheld Usability", Ed. John Wiley & Sons Ltd, New York, 2002.

[15] Tobii Eye Tracking. "Screen based eye tracking - Tobii T60 & T120". http://www.tobii.com/en/analysis-and-research/ global/products/hardware/tobii-t60t120-eye-tracker/, accessed May 2011.

[16] A. Duchowski. "Eye Tracking Methodology: Theory and Practice", Springer, 2nd edition, 2007.

 ISBN: 978-1-61208-164-9