

Critical Aspects In Authentication Graphic Keys

Sérgio Tenreiro de Magalhães¹, Kenneth Revett², Henrique M. D. Santos¹

¹ University of Minho
Department of Information Systems
Campus de Azurem
4800-058 Guimaraes, Portugal
{psmagalhaes, hsantos} @dsi.uminho.pt

² University of Westminster
Harrow School of Computer Science
London, UK HA1 3TP
revettk@westminster.ac.uk

Abstract: Some applications are using images instead of words as the user's authentication secret, in order to increase the number of possible keys (key's space), taking advantage of the several possibilities for each mouse click and of the fact that humans memorize images better than words. This paper presents the characterisation of the graphical keys chosen by almost 200 regular users of a website and the results show some important fact that must taken into account to maximize the security of the authentication process.

Keywords: Authentication; Graphic Keys, Passgraphs; Key Space; Key Characterization.

Introduction

The information provided by the arrested technological experts connected to terrorist groups resulted in the knowledge that these organizations are using the Web to communicate. Even more, the software found in their laptops showed that they are also involved in hacking activities, what can be seen as expectable once modern societies depend more and more on the stability of their technological infrastructures. So we need more reliable processes of authentication, the process of confirming an alleged identity. This differs from the identification process in which a user is linked to a known identity [Magalhães, 2005A]. In the Information Systems, authentication involves, traditionally, sharing a secret with the authenticating entity and presenting it whenever a confirmation of the user's identity is needed. In the digital era that secret is commonly a username/password pair and/or, sometimes, a biometric feature, both presenting difficulties of different kinds once the traditional pair user/password is no longer enough to protect these infrastructures, the privacy of those who use it and the confidentiality of the information (many of our countries secrets are hidden behind passwords), having known vulnerabilities, and the second has many issues related to ethical and social implications of its use [Magalhães, 2005B].

Password vulnerabilities come from their misuse that, in turn, results from the fact that they need to be both easy to remember, therefore simple, and secure, therefore complex. Consequently, it is virtually impossible to come up with a "good" password [Wiedenbeck, 2005]. On the other hand, once users have not yet completely realized the need for securing their authentication secrets, even fairly good passwords become a threat when the security policies (if at all existing) fail to be implemented. The results of an inquiry made by the authors in 2004 to sixty Information Technology (IT) professionals show that, even among those that have technical knowledge, the need for passwords security is underestimated.

Table 1 - The distribution of the passwords constitution shows a generalized vulnerability

Constitution of the passwords	Percentage of users
Letters and symbols	0%
Numbers and symbols	0%
Letters, numbers and symbols	17%
Only letters	23%
Only numbers	17%
Letters and numbers	43%

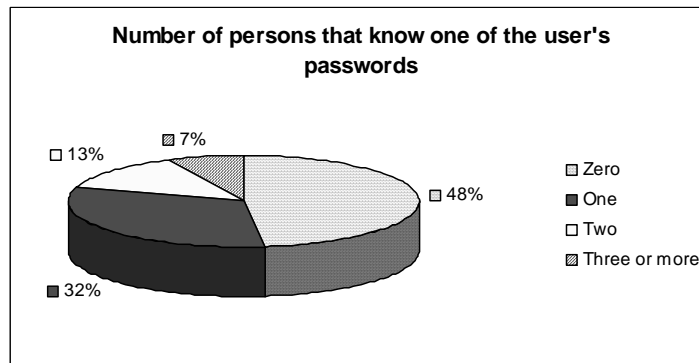


Figure 1 - Users have a generalized tendency to share their passwords

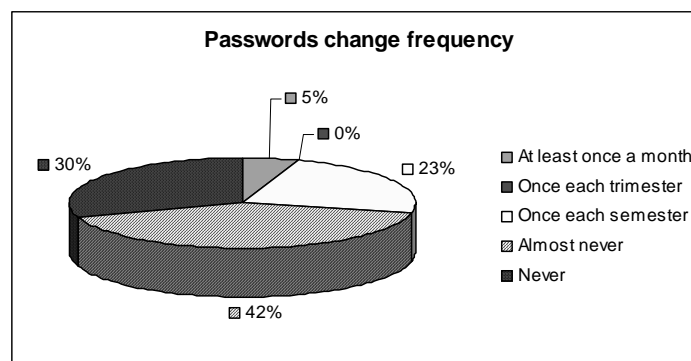


Figure 2 - Most of the users rarely change their passwords

As shown in the table 1, only 17% of the inquired professionals use complex codes including symbols, and 72% stated that they rarely change their access codes (Figure 1), despite 52% of them know that at least one of those is known by at least one other person (Figure 2). This need for simplicity and the principle of trust that allows a user to have the password on a post-it placed under the keyboard or even on the monitor, creates a security breach that can be stopped by graphical secrets (passgraphs), once they are easier to remember [Nelson, 1977] [Madigan, 1983], they can generate complex passwords (an easy way to assure easy compatibility with existing systems) and they are difficult to transmit from person to person. This need to stop the transmissibility of the authentication secrets is even bigger when we realize (Figure 3) that most professional users (65%) have only one or two codes that they use for authenticating to the generality of the used services.

Needless to say that the authentication processes based on passgraphs are, like virtual keyboards, adequate for use in private spaces or in small devices like the Personal Digital Assistants (PDAs), once they are vulnerable to eyesdropping. Giving to the user the possibility to choose at each login attempt between the passgraph mode and the password mode is also not a choice, once the system would inherit the vulnerabilities of both systems. So, the only

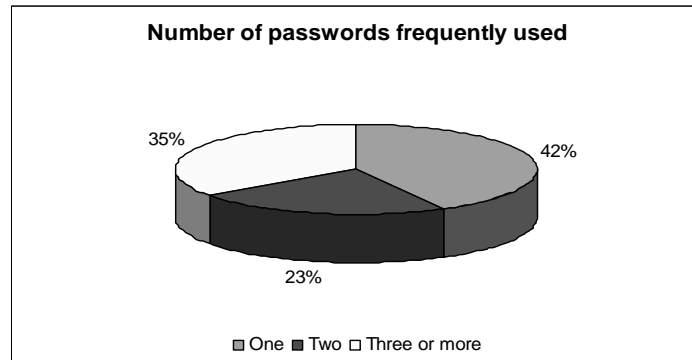


Figure 3 - Most of the users use the same password for accessing all services

way to implement this systems without limiting the users is to allow the user a choice between one of the processes when he uses the system for the first time (enrolment) and making that choice definitive (or almost). In this case, the user must be educated for the advantages and disadvantages of both systems so that he can make the choice that best suites is needs. In order to provide a useful widespread of passgraph systems they cannot generate new vulnerabilities. For this, it is essential that we can understand the users choices, so that we can use images that will maximize the entropy of the passgraph. This is, that will have regions with a probability of being chosen similar to the one resulting of a random choice. This paper presents a contribution to this knowledge of the users behaviour.

Previous work on passgraphs

Greg Blonder was the first to describe graphical passwords [Blonder, 1996], presenting in a United States Patent a system that would allow users to choose their picture, the number of regions to be clicked, their size and position. Since then, many variations of this system were presented and images have gained their way into the authentication processes.

Among the most popular graphical authentication systems we find PassfacesTM from the Passfaces Corporation, a commercial system where the user chooses a previously selected face from a set of faces and repeats this process for different faces in different sets for a defined number of times [PassfacesTM, 2005], but popular doesn't imply secure and a study of the users choices demonstrated that they are, in some cases, similar for all users. For instance, 10% of the passwords of males could have been guessed with only two attempts [Davies, 2004].

The *Déjà Vu* Scheme in which a matrix of m images is set, where n images are part of the user's portfolio, previously chosen from a set of proposed images. The user must identify those n images to login.

The *Draw A Secret* (DAS) scheme is a graphical authentication system with an approach completely different. In DAS the user draws something over a grid and that becomes is authentication secret. This system has been implemented with success in PDAs and further studies will be made to analyse the user's choices and acceptance [Jermyn, 1999].

In the Visual Identification Protocol (VIP) several possibilities were created. From a set of ten predefined images the user chooses four, placed on the same place and typed in the same order (VIP1) or placed in random positions (VIP2). VIP3 is a process where four of the eight images existing in the user's portfolio are displayed along with 12 distractors and the user must identify them in no particular order. The studies shown that the most common

errors associated with VIP1 and VIP2 were related with bad sequences, when the identified images are correct but selected on the wrong order, and in VIP3 most of the errors were due to wrong identification of the images, for instance any flower being consider as “the” chosen flower [de Angeli, 2003].

Description of the implemented system

Considering that the PDA is the technology that provides an environment that better takes advantage of the graphical authentication procedures and that the Word Wide Web is the most used distributed system, our system was designed to meet the authentication demands of a Mobile Web Service, especially web pages destined to be browsed in PDAs.

In order to test the authentication process in a real life situation we transformed the login procedure of the site of a graduation course normally protected by password, for copyright reasons and to protect the privacy of the students in matters like their grades, into a system protected by passgraphs. We use the Web Application Server PE 8, from SUN, for a regular file realm authentication invoked through a hidden field in a regular form. The created environment feeds this field with a string that results from the application of a function to the passgraph data. The security issues were then addressed in the same way that for a regular username/password authenticated site.

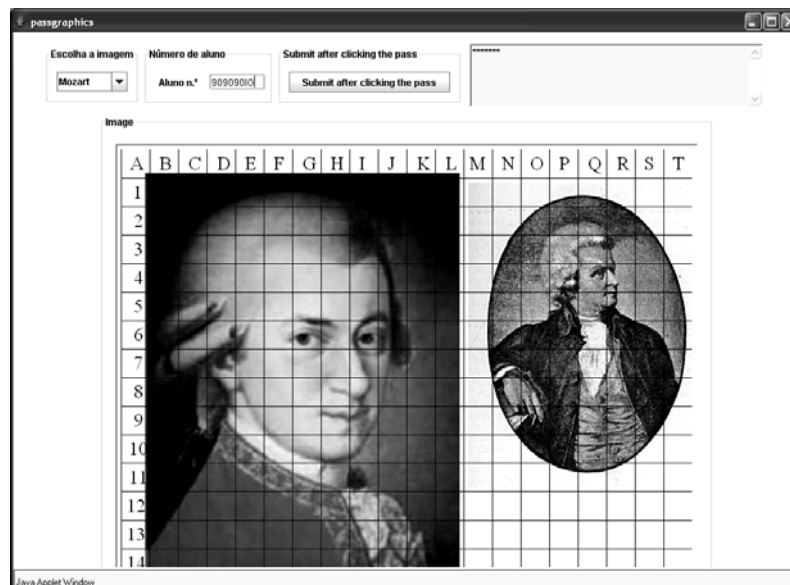


Figure 4 - The enrolment and authentication window

Both the enrolment and the authentication environment consist on a window with a field for a username, in this case the student number; a dialog panel, where the users get feedback from the system; and a select panel, where the user can choose the active image from a previously defined set. Each image includes a grid in which each area can be seen as a pair (letter, number) once the first line has the letters from A to T and the first column has the numbers from 1 to 14 and the letter A in the first position, equivalent to the line zero (Figure 4). This configuration was chosen in order to find out if the users would prefer a password scheme, instead of a graphical scheme. If this is so, the user will just pick a sequence of letters. On the other hand, this can also be used (with a full alphabet) for entering the username without the use of an external keyboard (virtual or physical). The user chooses an authentication secret by clicking on several points of the active image, which can be changed

at any time. The sequence of the picked points in the chosen images will be the authentication key for future logins. Once we are trying to fully understand the users free choices, no limitations were imposed to the length of the passgraph. In the dialog panel the symbol * appears whenever the user selects a region of the image, allowing it to know if he did in fact clicked or if he accidentally clicked twice. In this way we'll be able to reduce the number of login errors due to accidental clicks. In the final enrolment implementation, this panel will also transmit information about the limitations that will be made to the length of the passgraph.

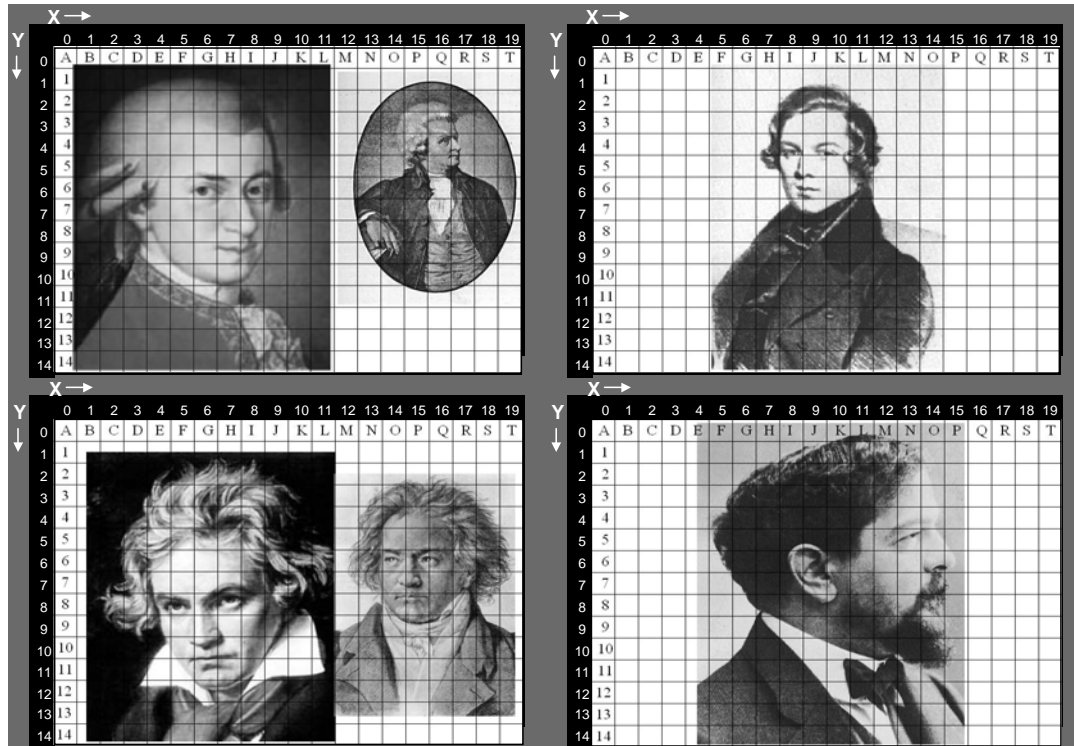


Figure 5 – The x and y axes on the four used images

The use of several images creates a third dimension factor once a passgraph with length n will be a vector of the type (p_1, p_2, \dots, p_n) where, considering I as the set of available images, $p \in \{(x, y, z) \mid 0 \leq x \leq 19, 0 \leq y \leq 13, 1 \leq z \leq \#I\}$. The values of x and y define the selected section in a specific two-dimensional image, as shown in Figure 5 for a set of four images (the ones used in our implementation).

Experimental results

In this section we present the practical results of this experiment, made on the 173 users choices of passgraphs. In order to have the users free choices, and therefore understand what are the users wills and derive a set of rules for future implementations, no limitations were imposed to the users.

From Figure 6 we can conclude that most of the users, almost two thirds, choose the first available image and that the lower an image gets in the picking lists the lower the probability of being chosen, reducing the entropy of the system once the ideal situation would be that every image would have the same probability. Being so, it's advisable that the images are presented to then users in a random order, both in the enrolment and in the authentication

processes. Also reflecting some laziness of the users is the fact that there were no users choosing a passgraph with clicks in different images. Unfortunately, we found no technical solution for this and, probably the way to improve these results is to educate the users.

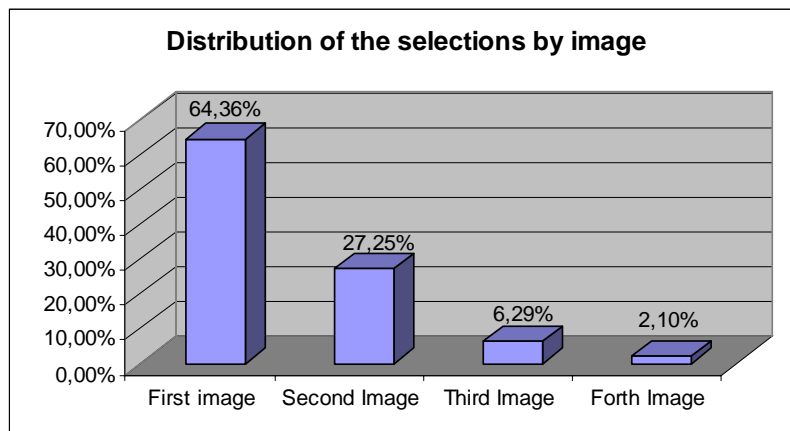


Figure 6 - Users tend to choose the images that are first presented to them

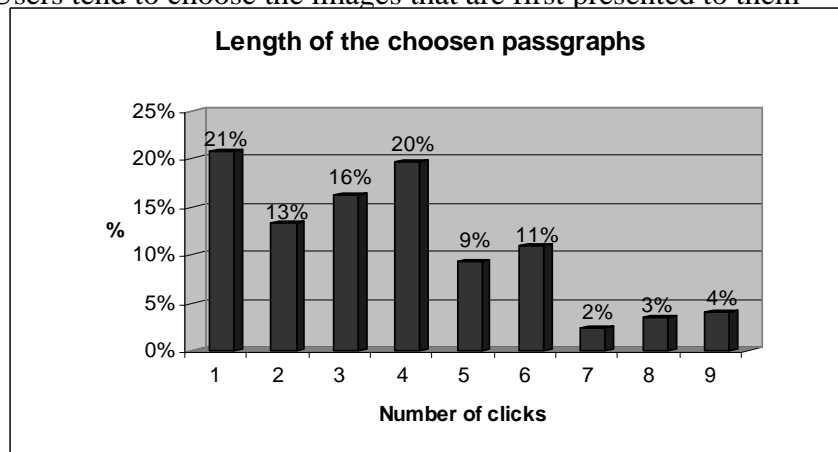


Figure 7 – 50% of the passgraphs have less then four clicks.

The average length of the chosen passgraphs is 3.9 clicks with 21% of the users having a passgraph constituted by only one click. This is clearly not enough and, therefore, our first rule for future implementations is that we must impose a minimum length in order to avoid the generalized vulnerability resultant from a widespread of short passgraphs. But, to force too many users to accept a passgraph bigger than the preferred one would generate a low acceptance of the system by the users, we consider that, al least in a first stage, we must define the minimum length in the size that will force 50% of the users to choose bigger passgraphs, this is (Figure 7), the minimum length will be set in 4 clicks.

Table 2 – Passgraphs constituted by numbers, characters or regions in the second line (right bellow the characters) are frequently found.

	Percentage of the users choices (%)
Passgraphs constituted exclusively by characters	6.36%
Passgraphs constituted exclusively by numbers	2.89%
Passgraphs constituted exclusively by regions in the line bellow the letters	10.98%

An interesting fact found in the users choices, for us unexpected, is the amazing percentage of users with passgraphs constituted by regions in the same line or in the same column. Over three quarters of the passgraphs (75.9%) are in one of these conditions, 55.5% with all the selected regions in the same line and 20.4% with all the selected regions in the same column. This tendency is even bigger in what concerns to the first column (passgraphs constituted exclusively by numbers) and to the first two lines, the one constituted by letters and the one right bellow (Table 2). This tendency can be contradicted a simple rule: the system must reject passgraphs that are constituted by regions in the same line or in the same column. This will force the users to navigate in the image and, therefore, increase the entropy of the chosen passgraphs.

Table 3 – The most common selected regions probability

	Expectable if random	Actual percentage
Regions in the line bellow the letters	6.67%	39.94%
Corners	2.11%	13.12%
Eyes	0.83%	9.18%
Letters	6.67%	10.06%
Numbers	5.26%	6.56%

Finally, as shown in the Table 3, we found that, besides the already solved tendencies like the letters or the regions in the line bellow them, some parts of the body are more chosen, the eyes, while others aren't, like the nose or the mouth. In fact, the probability of an eye region to be chosen (9.18%) is eleven times bigger than expected. This can only be solved by eliminating humans from the selected images or, in opposition, by using images that present so many eyes that the probability is dissolved between all of them. By looking at the Table 3 we also verify that the regions that are placed in corners are six times more chosen than expected if the distribution was random. So the images must be cut in a round way and they shouldn't represent objects with corners. All things considered we find that nature images are probably the most appealing for a safe use of passgraphs.

Conclusions

The main objective of the implementation of this system was to understand the users choices of images and of regions inside the images. The results show that the users have a common tendency to choose the first available images and that the use of images with corners and the existence of letters, placed in a row, creates serious vulnerabilities to the system. The eyes are also a common choice and should also be avoided. Therefore, the results suggest the use of images without corners, like natures, cut in a round form. In order to keep the letters, once they increase in a considerable way the comfort of use in PDAs, they must be placed in a random way throughout the images. Another dangerous tendency is the use of passgraphs constituted by regions placed in the same row or in the same column, therefore the system must reject the choice of passgraphs that meet this criteria, forcing the users to navigate inside the image by demanding the use of, at least, two different rows and two different columns. Passgraph systems have shown that they have potential to substitute, or complement, password systems but it is shown that, for that to happen, the web programmers must choose adequate images and implement the correct security policies.

Bibliography

Blonder, G. E.: *Graphical password*, U.S. Patent Number 5.559.961, 1996.

Davies, D., Monroe, F. and Reiter, M. K.: *On User Choice in Graphical Password Schemes*, 13th USENIX Security Symposium, 2004.

De Angeli, A., Coventry, L., Johnson, G.I and Coutts, M.: *Usability and user authentication: Pictorial passwords vs. PIN*, In P.T.McCabe, (Ed.). *Contemporary Ergonomics 2003* (pp. 253-258) London: Taylor & Francis, 2003.

Jermyn, I., Mayer, A., Monroe, F., Reiter, M.K. and Rubin, A.: *The Design and Analysis of Graphical Passwords*, Proceedings of the 8th USENIX Security Symposium, Washington, 1999

Madigan, S.: *Picture memory*. In *Imagery, Memory, and Cognition*, pages 65–86, Lawrence Erlbaum Associates, 1983.

Magalhães, S. T., Revett, K. and Santos, H. D.: *Password Secured Sites - Stepping Forward With Keystroke Dynamics*, Proceedings of the IEEE International Conference on Next Generation Web Services Practices, IEEE CS Press, Seoul, South Korea, 2005.

Magalhães, S. T. and Santos, H. D.: *An Improved Statistical Keystroke Dynamics Algorithm*, Proceedings of the IADIS Virtual Multi Conference on Computer Science and Information Systems, 2005.

Nelson, D. L., Reed, U. S. and Walling, J. R.: *Picture superiority effect*, *Journal of Experimental Psychology: Human Learning and Memory*, 3:485–497, 1977.

PassfacesTM: *The science behind PassfacesTM*, Passfaces Corporation, www.passfaces.com (Sept. 2005), 2005

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N.: *Authentication using graphical passwords: Basic results*, *Human-Computer Interaction International (HCII 2005)*, Las Vegas, July 25-27, 2005