A Multi-Grid Graphical Password Scheme

Konstantinos CHALKIAS, Anastasios ALEXIADIS, George STEPHANIDES

Dept. of Applied Informatics, Macedonia University,
156 Egnatia str., 540 06 Thessaloniki, Greece
chalkias@java.uom.gr, talex@java.uom.gr, steph@uom.gr

Abstract. The vast majority of computer and communication systems use passwords in order to identify users. Unfortunately, in ubiquitous alpha-numeric password schemes, users tend to choose passwords with predictable characteristics, related to how easy they are to remember. To overcome the vulnerabilities of textual passwords, a lot of alternative techniques have been proposed such as visual or graphical login, biometric systems and fingerprint verification. In this paper we focus on graphical password techniques and more specifically we make an extension to the Draw-a-Secret scheme (DAS) proposed by Jermyn et al. (1999). On the simple DAS scheme the user draws a design on a display grid, which is used as the password. Motivating by the fact that users tend to draw lines and shapes on specific areas in the grid, we propose a different multi-grid construction of the DAS technique. By making a survey on a sample of people with different age and technical knowledge, we concluded that this approach increases the password strength, while remaining user-friendly.

Keywords: password identification, system identification, DAS technique

Math. Subjects Classification 2000: 93B30, 92E12, 65M55

1 INTRODUCTION

The role of a user authentication mechanism is to provide the means for a secure access to sensitive information. The authentication mechanisms are divided into three classes of procedure [5]: " Proof by knowledge: the user's claimed identity is established through information that can only be produced by the user itself (e.g., a password). " Proof by possession: the user's claimed identity is established through the possession of an object associated with and exclusive to that identity (e.g., a smart card). " Proof by property: the user's claimed identity is established through the direct measurement of certain properties (i.e., biometrics), which match those of the user with that identity (e.g., a fingerprint). Until now, most of the authentication systems are based on alpha-numeric passwords (proof by knowledge). Their wide use is due to the low implementation cost and the ease of use. The main disadvantage of this kind of schemes is that users tend to choose passwords with predictable characteristics, related to how easy they are to remember. The latter means that memorable passwords typically exhibit patterns and they fall into a small subset of the full password space. In a case study conducted by Klein [8], 25% of 14000 passwords were cracked using a dictionary of only 3 million words. Another fact that proves the weakness of textual passwords is the remarkable success ratio of the Morris Worm [13][14]. This Worm used a dictionary of 432 words in addition to the 1988 UNIX online dictionary (about 25000 words] and some sites reported that 50% of their passwords were correctly guessed. These facts prove that textual password-based authentication systems are susceptible to automated dictionary attacks. In order to overcome the vulnerabilities of textual password schemes, new innovative password schemes had to be found. The trend toward a highly mobile workforce has spurred the acquisition of notebook computers and handheld devices such as Personal Digital Assistants (PDAs) at an even increasing rate. These devices support a set of interfaces that are oriented toward user mobility and they usually come equipped with a touch-pad or a touch-screen. This kind of equipment motivated researchers to propose different user-friendly password schemes that require recall or creation of a picture (visual and graphical login). In this paper we focus on graphical password techniques and more specifically we make an extension to the DAS scheme proposed by Jermyn et. al [7]. On the simple DAS scheme the user draws a design on a display grid, which is used as the password. This design may include block text as well as graphical symbols and shapes. Motivating by the fact that users tend to draw lines and geometrical shapes on specific areas in the grid, we propose a different construction that uses nested grids. By conducting a survey on a sample of people with different age and technical knowledge, we concluded that this approach increases the memorable password space, while remaining user-friendly. We also implemented an application that users are encouraged to use different pre-defined grid templates according to their needs and their password choice and the results show that this approach is suitable for less technical inclined people, as it helps them create more complex password representations. The rest of the paper is organized as follows: §2 provides information about existing visual and graphical password schemes (including a detailed description of the simple DAS scheme). In §3 there is a reference to the proposed multi-grid DAS scheme. In §4 there is the full description of the user study and its results. Finally, concluding remarks and future work are discussed in §5.

2 RELATED WORK

Graphical and visual logins are knowledge-based approaches that take advantage of the device's built-in display and image selection or drawing capabilities. Suo et al. [16] conducted a survey related to graphical and visual passwords and they categorised the graphical schemes into two basic classes, the recognition-based and the recall-based schemes. Monrose and Reiter's overview of graphical passwords [9] provides a slightly different categorization. The recognition-based class refers to mechanisms that rely on the selection of pre-defined images to produce a password value. Instead of alpha-numeric characters, users must remember image sequences. An authentication system of this class is the Déja Vu, which was developed by Adrian Perrig and Rachma Dhamija[3]. In this scheme, a user selects a set of images that form his portfolio set. Then, at login phase, the user is shown a randomly generated set of images called the challenge set. The challenge contains some images of the user's portfolio set. For a successful login, the user has to select the images that belong to his portfolio. Another recognition-based scheme called Passfaces[12] is based on a human's ability to remember and recall faces from a random set of face-images. A similar approach is called Story and the only difference with the Passfaces technique is that it uses a variety of photo categories (e.g., food, cars, animals, and people), and the user is asked to create a story to help him remember his portfolio. Some other efficient password schemes that belong to this category were proposed by L. Sobrado and J.-C Birget[15]. The two authors tried to solve the shoulder surfing problem (watching over people's shoulders as they process information) by adapting challenge response authentication techniques to graphical passwords. Among their proposals there are two very promising schemes, the Triangle scheme and the Movable frame scheme. In the first case, the user pre-selects a set of K images and then the system randomly scatters a set of N images on the screen. To login, a user must find three of his pass-images and click inside the invisible triangle created by those three images. In the second case, only three pass-images are displayed on the screen and only one of them is randomly placed in a movable frame. The task of the user is to move the frame, by dragging the mouse around it, until the pass-image on the frame lines up with the other two pass-images. Recall-based schemes can be divided into two sub-categories. In the first category, systems where a user has to click on several points on an image are included. Several schemes of this class have been proposed [5][6][18], such as PassPoints[18] where a user has to click relatively close to some points on an image to gain access to the system. The second category includes schemes that rely on the creation of graphical images to produce a password value. Jermyn et al. proposed a scheme called Draw-a-Secret (DAS), targeted for PDA devices. In this scheme, the user draws a design on a display grid, which is used as the password. The design may include block text as well as graphical symbols. The main difference from graphical pattern recognition is that DAS passwords must be exactly repeatable. The latter means that strokes can start anywhere and go in any direction, but must occur in the same sequence, as the one in the registration phase. To produce a password, each continuous stroke is mapped to a sequence of coordinate pairs, by listing the cells through which it passes, in the order in which it traverses the cell boundary. Exact repetition allows for the password to be stored as the output of a one-way hash function. To avoid ambiguity in cases of strokes that run along the cell boundaries, the size of each cell must be sufficiently large to provide a degree of tolerance when the user draws a password. Jermyn et al. suggest that the size of the password space for graphical passwords formed using a 5 × 5 grid is larger than that of alphanumeric passwords. Figure 1 illustrates a four-stroke password entry.

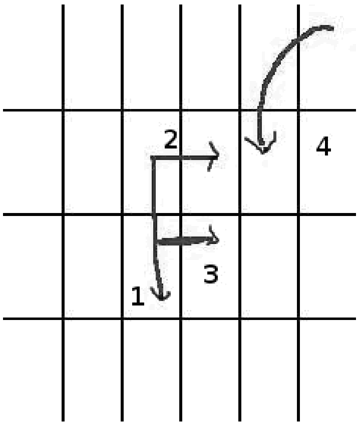

Fig. 1. DAS password example (4 × 6)

There have been a number of analyses of graphical passwords in terms of their memorability. Jermin et al. [7] suggest that the security of graphical password schemes benefit from the current lack of knowledge of their probability distribution. The latter motivated J. Thorpe and P.C van Oorchot [17] and D. Davis et. al [2] to propose classes of memorable graphical passwords by examining what types of pictures people recall better. A separate user study from Goldberg et al.[4] showed that people are less likely to recall the order in which they drew a DAS password than the resulting image. Moreover, a survey conducted by D. Nali and J. Thorpe[10] showed that people tend to choose passwords with predictable characteristics and the majority of them uses centered or approximately centered passwords (meaning centered about a set of cells adjacent to the center grid lines). There have been some attempts to improve the memorable password space and the performance of the simple DAS. Birget et. al[1] proposed a different construction that uses multi-grid discretization. In this scheme three grids are used in order for a point to be at safe distance from the edges from at least one of the three grids. This approach is suitable in cases where the strokes pass through the corners of the cells. Another idea was proposed from P.C van Oorschot and J.Thorpe[11]. They suggested that increasing the grid size to increase the password space does not provide enough security pay-back as increasing other parameters, such as stroke-count or password length. Under their assumption, they proposed a scheme that uses grid selection, in which a user selects a small drawing grid from an initial large, fine-grained grid. Their idea is similar to that discussed by Birget et al. (2003), except that they are zooming in on a grid to draw in, not a picture to click a point within.

3 PROPOSED MULTI-GRID DAS

Analysing the results of the survey conducted by D. Nali and J. Thorpe[10] we can understand that the password centering effect could make the DAS passwords vulnerable to attacks. More precisely, the survey showed that 86% of the users drew a centered or approximately centered password. Furthermore, 45% of the passwords were totally symmetric and 29% of the passwords were invalid (strokes cross the cell corners or follow the grid lines). Figure 2 illustrates an example of a centered password. As it is already referred in the previous section, GoldBerg et. al [4] conducted another user study to compare the text-password login success ratio with that of the DAS password login success ratio. The results showed that about 58% of the users recalled their text-passwords correctly and 52% of them successfully recalled their DAS passwords. Another interesting result of this survey was that too many users forgot their stroke order.

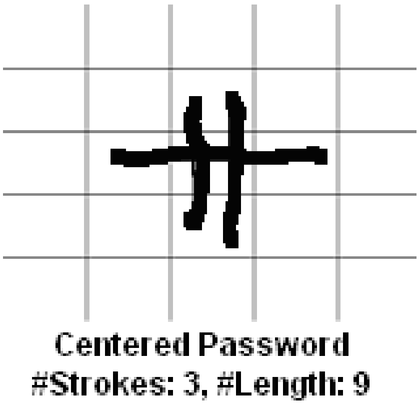

Fig. 2. Centered password example (5 × 5)

As it can be easily seen, users tend to draw passwords with predictable characteristics. It seems that users choose specific areas of the grid to draw their password. The centering effect shows that there is a high probability for a password to be near the absolute middle of the grid. To overcome this vulnerability, we propose a different modified DAS scheme where the cells are not identical in size. Our idea can be easily implemented using a multi-grid construction. The final grid could be composed from several internal grids.

The aim of our proposal is to decrease the password centering effect. In this multi-grid case, the user is able to focus in a single internal grid, so there is more than one area where the password can be centered to. Figure 3 illustrates an example of a multi-grid graphical password.

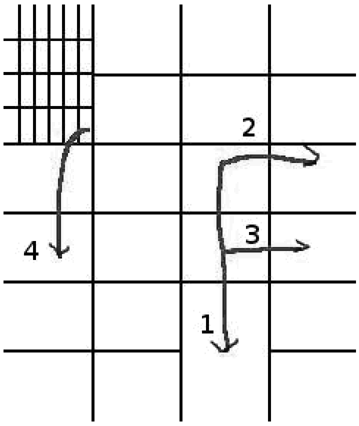

Fig. 3. A multi-grid password example

Another advantage of the proposed scheme is that the existence of a lot of visual base points can decrease the invalid-password ratio. The main reasons that users fail to repeat their password is the fact that they forget their stroke order or they mark adjacent cells and not the correct ones. The errors that belong to the first category are called ordering errors, while the errors that belong to the second one are called shift errors. An example of a shift error can be seen at Figure 4.

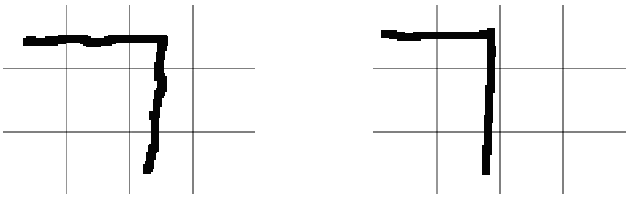

Fig. 4. A shift error

As it has been referred above, most of the users draw one to three strokes. In real world cases the user has three to five attempts to draw the correct password. In case of an ordering error we expect that five retries are usually enough to find the correct password (if the stroke count is less than three). However, in case of a shift error it is less possible to find the correct drawing especially when the size of the grid is big enough (e.g., 10 × 10). The latter means that is very important to find a way to decrease the shift error ratio. We suppose that the multi-grid approach will decrease the shift errors as the full grid consists of small nested grids. The results of our survey presented in the next section suggest that multi-grid approach really eliminates the shift errors. Another important factor of security when using multi-grids is that the user has the opportunity to choose a grid from a list of pre-defined multi-grid templates. In this case, every user will have his custom grid which means that an attacker has to try even harder to find a password using massive brute-force techniques. This is caused to the fact that the number of the neighbour cells is not fixed. In the simple DAS approach every cell has at most four adjacent cells. In our approach a cell can have more than four neighbours as it can be seen from Figure 5 where the cell in the absolute middle of the grid has eight neighbours.

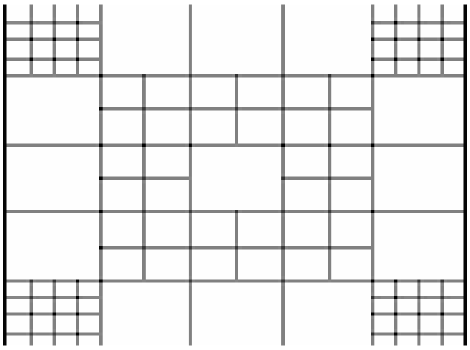

Fig. 5. A complex multi-grid template

4 SURVEY DETAILS AND RESULTS

In order to compare our multi-grid approach with the simple DAS and the text-password schemes respectively, we conducted a survey on a sample of 30 people. The sample consisted of 15 children that go to the primary school (6-11 years old) and 15 computer-related university students (19-27 years old). The reason of this distinction was due to the fact that we wanted to compare the results of non-technical inclined people with that of well-informed people. At the beginning of the survey, specific instructions were provided to the students. We made a short course of about 25 minutes explaining the text-based approach and the graphical password technique. Moreover, we presented some basic password examples and we analysed some of the graphical password features such as the cell marking, the password complexity and the difficulties in password representation and recalling when drawing-lines pass through the corners of the cells as well as when passing along cell boundaries. The survey had two phases. The registration phase and the login phase. In the first phase the participants were asked to create the three passwords (a textual-password, a DAS password and a multi-grid graphical password) in a specific memorable way by entering it at least for four times to increase the possibility of password matching. Following a one-hour break and short interview to obtain information about their past computer experience; in the login phase, users were asked to recall their graphical passwords. Concerning the grid size, we used a 4 × 6 grid for the simple DAS, while for the multi-grid system we used a nested grid with 21 cells as the one illustrated in Figure 6. We tried to use grids with similar characteristics to provide fairness when examining the results of the user study. We consider a password match if it is drawn exactly as the password entered at the registration phase. Criteria for a match in graphical passwords include the number of strokes, the order and direction of strokes and the password length.

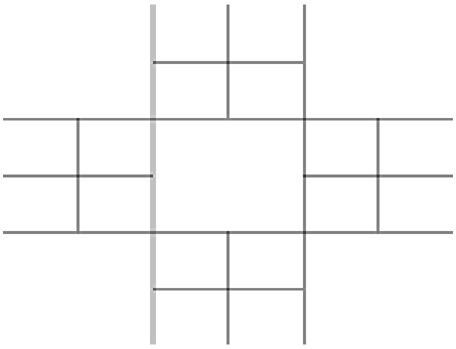

Fig. 6. A multi-grid template

To compare the simple DAS scheme with the proposed scheme, the results were categorised for the following characteristics: number of strokes, password length, centering within the grid (centered, approximately centered, or not centered)[10], matched passwords, visual matched passwords (only ordering errors) and shift errors. For the textual-passwords we needed to measure the matched passwords and the number of characters used (password length). In order to compare the results of technical and non-technical users we present the tabular data for both user classes. Table 1 represents the results for textual-passwords, Tables 2 and 3 represent the results for the simple DAS scheme and Tables 4 and 5 represent the results for our proposed multi-grid scheme.

Table 1. Textual-password results

	Matched	**Average Length**
Non-technical	66%	4.5 Characters
Tech	80%	7.2 Characters

The results of the textual-passwords showed that non-technical inclined people choose very small text passwords that are easy to be cracked. Moreover, most of the children (about 67%) used only numbers as passwords and none of them used mixed numbers and characters. As for the university students, 26% used only numbers, while 40% used less than 6 characters.

Table 2. DAS password results

	Matched	**Ordering errors**	**Shift errors**
Non-technical	47%	20%	33%
Technical	60%	20%	20%

Table 3. DAS password complexity

	Num. of Strokes	**Average Length**	**Centered**
Non-technical	2.9	8.5	80%
Technical	3.6	9.7	67%

The results for the simple DAS technique show that less than the half of the students of primary school recalled their password correctly. Although the results for the technical inclined people were a bit better, the match ratio is still smaller that the textual-password approach. Concerning the password centering effect, we can see that the majority of people, especially the non-technical ones, choose predictable centered or approximately centered DAS passwords. Surprisingly, the user study for the multi-grid approach showed that the password match ratio has been increased, while the shift errors have been eliminated to 13% for both user classes. As for the ordering errors and the password length, it seems that there is no big difference from that of the simple DAS approach. Additionally, the results for the centering effect are very promising, as in our proposed approach the centered passwords has been decreased to less than 50%. The latter makes our scheme more resistant to graphical dictionary attacks.

Table 4. Multi-grid password results

	Matched	**Ordering errors**	**Shift errors**
Non-technical	60%	27%	13%
Technical	67%	20%	13%

Table 5. Multi-grid password complexity

	Num. of Strokes	**Average Length**	**Centered**
Non-technical	3.0	8.4	46%
Technical	3.3	9.5	33%

5 CONCLUSIONS AND FUTURE WORK

The multi-grid extension of the DAS graphical password scheme enables users to center their passwords in different areas on the grid. The user study presented supports that the use of nested grids provides better security while remaining user-friendly. Our proposed scheme reduces the number of shift errors, while the results of the ordering errors stay unchanged. We expect that the selection of custom grid-templates will give much better results. The latter will make this scheme even more resistant to dictionary attacks than the simple DAS approach. We are currently working on techniques that improve the security of graphical passwords and increase the memorable password space. One way to do that is to color specific areas in the grid, so users will focus in their password area much faster. Another improvement would be to combine picture passwords with graphical passwords by using a background image in the grid area. Finally, an open task is the implementation of grid-agents that will propose the appropriate grid template according to the user's password.

References

[1] **J.-C. Birget, D. Hong, N.Memon**, Robust discretization with an application to graphical passwords, Cryptology ePrint Archive, Report 2003/168; http://eprint.iacr.org (May 2006).

[2] **D. Davis, F. Monrose, M.K. Reiter**, On user choice in graphical password schemes, In *13th USENIX Security Symposium*, 2004.

[3] **R. Dhamija, A. Perrig**, Déja Vu: a user study using images for authentication, In *9th USENIX Security Symposium*,2000.

[4] **J. Goldberg, J. Hagman, V. Sazawal**, Doodling our way for better authentication, CHI '02 extended abstracts on Human Factors in Computer Systems,2002.

[5] **W. Jansen** Authenticating users on handheld devices, In the *Canadian Information Technology Security Symposium*, 2003.

[6] **W. Jansen, S. Gavrila, V. Korolev, R. Ayers, R. Swanstrom**, Picture password: A visual login technique for mobile devices, NISTIR 7030, http://csrc.nist.gov/publications/nistir/nistir-7030.pdf, (2003).

[7] **I. Jermyn, A. Mayer, F. Monrose, M. Reiter, A. Rubin**, The design and analysis of graphical passwords, In *8t h USENIX Security Symposium*, 1999.

[8] **D. Klein**, Foiling the Cracker: a survey of, and improvements to, password security, In *2nd USENIX Security Workshop*, 5-14, 1990.

[9] **F. Monrose, M.K Reiter, Graphical Passwords. In** *Security and Usability*, L. Cranor and S. Garfinkel, Eds. O'Reilly, Chapter 9, 147-164, 2005.

[10] **Nali and J. Thorpe**, Analysing user choice in graphical passwords, Tech. Report TR-04-01, School of Computer Science, Carleton University, Canada, 2004.

[11] **P.C. van Oorschot, J. Thorpe**, On the Security of Graphical Password Schemes, Technical Report TR-05-11. Integration and extension of USENIX Security 2004 and ACSAC 2004 papers, 2005.

[12] Real User Corporation, About passfaces, http://www.realuser.com/cgi-bin/ru.exe/_/homepages/technology/passfaces.htm, (accessed May 2006).

[13] **E. Spafford**, OPUS: Preventing Weak Password Choices, *Comp. Secur.* 11, 3, 273-278, 1992..

[14] **E. Spafford**, Crisis and aftermath (The internet work), *Comm. of the ACM* **32(6)**, 678-687, 1989.

[15] **L. Sobrado, J.C. Birget**, Graphical passwords, The Rutgers Scholar, vol.4. http://RutgersScholar.rutgers.edu/volume04/contents.htm . (2002).

[16] **X. Suo, Y. Zhu, G.S Owen**, Graphical Passwords: A Survey, In *21st Annual Computer Security Applications Conference (ACSAC)* (December 5-9), 2005.

[17] **J. Thorpe, P. van Oorschot, Graphical dictionaries and the memorable space of graphical passwords**, In *13th USENIX Security Symopsium*, 2004.

[18] **S. Wiedenbeck, J. Waters, J. Birget, A. Brodskyi, N. Memon, Passpoints: design and longitudinal evaluation of a graphical password system,** *International J. of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security)* **63**, 102-127, 2005.