American Journal of Applied Sciences 11 (7): 1065-1069, 2014
ISSN: 1546-9239

doi:10.3844/ajassp.2014.1065.1069 Published Online 11 (7) 2014 (http://www.thescipub.com/ajas.toc)

GRID-IMAGE PASSWORD BASED SCHEME: ENHANCING MEMORABILITY FEATURES OF PASSWORDS

[1]Obasan Adebola, [2]Norafida Ithnin and [3]Mohd Zalisham Jali

[1,2]Information Assurance and Security Research Group,
Department of Computer System and Communication,
Faculty of Computing, Universiti Teknologi Malaysia, Malaysia, Skudai, 81310 Johor, Malaysia
[3]Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Bandar Baru Nilai, Negeri Sembilan, Malaysia

Received 2012-10-30; Revised 2013-03-04; Accepted 2014-07-28

ABSTRACT

Password authentication has become a widely recognized element of computer security practices where human users are proven or confirmed as legitimate users for access to secure systems. Using this system, every user needs to recall its password correctly before access can be granted to an intended services or applications. Remembering the secure passwords is an everyday problem for users because of individual memory limitation. In an effort to solve this problem, graphical password was presented as one promising athentication alternative taking advantage of picture superiority over texts. The main objective of this study is to provide a comprehensive survey of array of graphical password schemes in different categories based on their common features with the primary aim of identifying the memorability features and propose a new graphical authentication system with enhanced memorability features.

Keywords: Graphical Passwords, Password Space, Authentication

1. INTRODUCTION

Computer security is a critical issue with modern information systems because its valuable contents and diverse day-to-day applications, namely banking, accounting and others. Consiquently, they require some measures of control and protection to ensure reliability, integrity and other security goals. In order to achieve reasonable level of protection, username-password methods have been widely used as method of choice for identifying, authenticating and authorizing users by many banks, government and corporate bodies and even all websites on the internet. The user identification is employed to identify a user to the system while the authentication proves user's claimed identity as being right or wrong depending on username and corresponding password. In order to complete used authentication process, authorization deals with the users' right to access resources ones they are authenticated. Text-based password method was introduced in the 1960s as a security measure to restrict access of useful information to authorized users within a computer system setup or worldwide networked computers (Nielsen and Vedel, 2009).

Conversely, it is popularly known that text passwords are vulnerable and insecure for a number of problems (Biddle *et al*., 2012; Lashkari *et al*., 2009). For this reason, other factors are used to complement and improve the security of text password mechanisms (Karnan *et al*., 2011; Tiwari *et al*., 2011; Vu *et al*., 2007). The main problems of text-based passwords is that users find it difficult to remember secure passwords which are expected to be meaningless strings choosen from lower and upper case letters, digits and special symbols (Zhang *et al*., 2009). Intensive studies in this area have revealed that users tend to pick short passwords or passwords that are meaningful in favour of memorability (Biddle *et al*., 2012; Vu *et al*., 2007). Unfortunately, such meaningful strings are weak text passwords which can be easily guessed or broken, by an attacker who strives maliciously to obtain the legitimate user passwords through dictionary, keystroke logging,

Corresponding Author: Obasan Adebola, Information Assurance and Security Research Group, Department of Computer System and Communication, Faculty of Computing, Universiti Teknologi Malaysia, Malaysia, Skudai, 81310 Johor, Malaysia

phishing, eavesdropping, shoulder surfing and other threats (Bonneau, 2012; Forget *et al*., 2010; Hafiz *et al*., 2008; Owens and Matthews, 2008).

Moreover, another easy method that can be used to restrict access of information to the legitimate users through knowledge-based authentication mechanism which does not require additional hardware is graphical passwords where pictures are drawn via mouse or stylus to register passwords instead of texts to lessen the passwords being forgotten. This advantage is caused by the capability of humans memory which retains graphical representations longer than texts. In 1996, the idea of Graphical passwords was conceaved by Blonder as an alternative to text-based password for user identification (Almuairfi *et al*., 2011; Chiasson *et al*., 2007; Zhang *et al*., 2009). In this system, an image appears on the screen, then user clicks with the help of mouse or stylus on one or more chosen regions of the displayed image to create a password. A user can only be authenticated if correct regions are clicked at later stage.

1.1. Graphical Password Authentication Systems

Today, many graphical password systems which require use of visual information to identify users are available in many forms and to some extent, they provide features required to overcome passwords memorability problem for users in user-friendly environments provided by the same graphical systems (Almuairfi *et al*., 2011). This is possible due to psychological theories that humans have a momentous competence to recall and to recognize visual information or images. In addition to making passwords easy to remember, graphical password methods must provide desirable level of security to resist some basic attacks such as dictionary and brute attacks, an attacker must construct a bigger dictionary than conventional textual passwords before these attacks can be successful (Zhao and Li, 2007).

Over the last decade, several graphical password systems have been proposed with intensive studies on them. The available graphical password schemes are categorized in diverse forms. Table 1 below discusses a number of schemes that are relevant to our study in two categorizations. In a grid-based graphical system, user typically draws and reproduces their password on a drawing grid to verify its identity (Nali and Thorpe, 2004; Tyagi *et al*., 2011). This approach is alphabet independent and as such making it equally accessible for users of any language (Jermyn *et al*., 1999). These systems exist in different forms as illustrated in Table 1 below. The **Figure 1** shows Drawing-A-Secret (DAS) scheme. Other implementation alternatives of DAS scheme (Chalkias *et al*., 2006; Lin *et al*., 2007; Tao and Adams, 2008; Thorpe and Van Oorschot, 2004) are also represented in **Fig. 1**. While in an image-based graphical system, users typically draw and reproduce their passwords over some portion or the entire picture/image for the purpose of authentication. These systems are in different forms (Wiedenbeck *et al*., 2005) as illustrated in Table 1. PassPoints system is the image-based scheme adapted in our scheme and illustrated in **Fig. 2**. Where it was shown that a PassPoints password is a number of points, selected by a user in an image that is displayed on the screen.

1.2. Merits and Demerits of Grid-Based Graphical Passwords:

- Grid of size NxN is a simple and ordered structure consisting of equal cells and each cell is denoted by two-dimensional discrete coordinates (x,y) which is a member of [1,N]x[1,N]
- Grid-based systems are recall-based algorithms, as such they rely on users' memory to provide the passwords correctly, without any cue from any image if background image is not provided
- A user study conducted by reaveled that it is difficult for users to draw their passwords with mouse or stylus in 2D grid coordinates and maintaining the sequence at the same time
- Perfect drawings with mouse or stylus without comiting fussy boundary prolem is difficult
- Identifying the starting point for some drawing may be hard

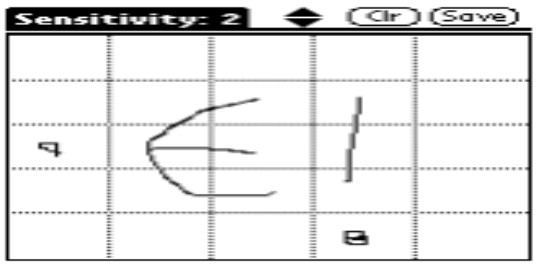

Figure 1. DAS Graphical scheme

Figure 2. Every pixel on an image used in the PassPoints system can be used for the password

Table1. Illustrating summary of existing schemes

Grid-based schemes	Image-based schemes
Drawing-A-Secret (DAS), is the first of its kinds. It was developed by Jermyn in the year,1999 as a graphical passwords on grid background. In this system, passwords are pictures drawn on cell of a 5×5 grid and identified by their coordinates of the cells.	In 1996, Blonder pioneered the idea of graphical passwords scheme. In this scheme, the user clicks with a mouse or other device like stylus on a few chosen regions in a single image-based background that appears on the screen and a password is a number of clicks on these locations in a particular order. The scheme was limited to one pre-proccessed image.
Passdoodle algorithm was proposed by Christopher *et al*. (2004). The scheme was based on the idea of hand written designs or words, drawn with a pen onto a sensitive screen. Users are validated by tracing a doodle over a touch screen, which is then accepted or rejected by the system.	Dhamija and Perrig (2000) proposed Déjà Vu system for the purpose of user authentication based on Hash Visualization technique. Its design involved the use of random or non-describable abstract images, rather than photographs. In this scheme, the user selects a specific number of images from a larger set of images presented by a server. The user has to identify the pre-selected images for him or her to be authenticated.
In 2004, grid selection was proposed by Thorpe and Van Oorschot to strengthen security and increasing the size of password space of DAS technique. The method together with zoom feature enable the user to select a drawing grid. In this technique, a large scale grid is offered and a user is required to choose a small drawing grid and then draw the password.	Passpoint is scheme that uses any kind of image provided by the system or chosen by user as an improvement over Blonder's scheme. This authentication scheme was developed by Wiedenbeck *et al*. (2005). In Passpoints, the image gives a cue and provides large password space.
Multi-grid scheme was designed by Chalkias *et al*. (2006) as an improvement of DAS. In this scheme, grid-squares not identical in size and shape, where user draws a design on a display grid whose coordinates are used as the password. The aim of this schemeis to decrease the password centering effect and to increase the password strength in user-friendly environment of the scheme	Passlogix V-GO system is one of password schemes based on the Blonder's technique developed by Passlogix and Microsoft in large scale. To create a password with V-GO, a user can click on a number of items in a single image in a particular sequence.
Pass-Go was motivated by an old Chinese game, Go. The scheme was proposed by Tao in 2006 as an improvement of the DAS. User selects intersections instead of cells on a 9*9 grid as in the case of DAS. The use of intersections as against cells allows the user to use password from greater password space (256 bits for the most basic scheme) and provides better usability than DAS.	"Passfaces" is a graphical password technique developed by Real User Corporation. In the scheme, the users are expected to choose just any four images of human faces from a face database as their future password. The user is authenticated if he/she correctly identifies the four faces in four different rounds.
Qualitative Draw-A-Secret (QDAS) was made by Lin *et al*. (2007) as an improvement of DAS to solve shoulder surfing (Tyagi *et al*., 2011). QDAS introduces qualitative spatial descriptions of strokes and the use of dynamic grid transformations that distinguish it from its DAS counterpart. With these features, users could set strong secrets that do not impose load on long-term memory and to be resistant to shoulder surfing.	Story scheme was proposed by (Davis *et al*., 2004) is an improvement over passfaces. In Story's scheme, a user's password is a sequence of k images selected by the user to make a story. The scheme offered better security because user select random images that not related to them unlike human faces.

- They are vulnerable to shoulder surfing attack when used in an open place
- The password space is almost infinity in DAS. The total number of possible passwords is larger than that of image-based systems

1.3. Merits and Dismerits of Image-Based Graphical Passwords

- Conducted study reveals that image-based schemes are very easy to remember due to the fact that users have competency to remember images. Image-based methods provide superior set of memorability features, especially those ones that make meaning to users
- Users could be biased in making their passwords which was highly influenced by their gender, race and attractiveness of image in use
- A low-detail image could have scanty clickable points which ultimately results to small password space making the system vulnerable to password brute-force and guessing attacks. While an image with high-detail scene has hundreds of clikable points which translate to larger password space and make a chosen password difficult to guess and observe
- Image-based graphical passwords require techniques for controling the tolerance error in order to avoid mis-selected click points or passwords and to have an efficient system
- Every image has some regions that are more attractive than the others and user tend to click on such regions to form their passwords. Any image with too many attrative locations may cause hotspot, dictionary and targeted attacks

1.4. Proposed Scheme

To enhance graphical passwords, we have developed a system grid-image-based graphical password system. The system involves two 5×5 matrices which adapted from image and grid-based methods and the technique is aiming at enhancing the graphical authentication in terms of memrability and better security by reducing the posibility of occurrence of shoulder surfing problem. Our adaptation is influenced by taking the merits of both methods and

possibility of enhancement. This new system involves two main steps, namely registration and authentication phases and each phase has activities that should be peformed. In the first step, users are required to select one event from a list of ten everyday events which then appears over the grid. The event provides autobiographical memory (Adebola *et al*., 2013) which serves as a cue to see whether users can set more complicated passwords and to know whether the event helps user to remember them during authentication phase (Dunphy and Yan, 2007). The grid divides the image into 5×5, which is 25 parts where passwords are drawn. In the second step of this phase, users enter their username and click their passwords on the grid, then save the passwords to a MySQL database over an extended period of time. **Figure 3** illustrates the activities during registration phase.

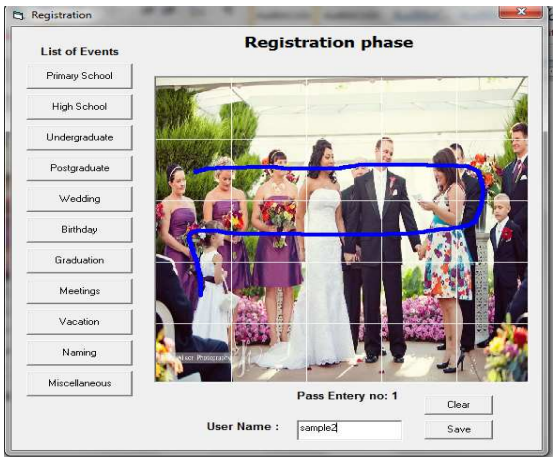

Figure 3. The registration phase grid showing 10 events with user chosen event and passwords

Figure 4. The authentication phase grid depicting user chosen event, password digits, decoy digits and on-screen pad

During the login process, the user will be presented with **Fig. 4** from the database after entering the usename correctly. The user enters any five cells corresponding to his/her passwords via on-screen pad without touching the screen to avoid shoulder surfing because the image in the grid and passwords are directly seen by anxious and malicious observers when they are being used. **Figure 4** illustrates a user entering "24533163613" from the randomly generated digits as his password. The passwords selected must correspond to the selected cells highlighted in **Fig. 4**. Once that happens the login is successful otherwice the login is unsuccessful.

2. CONCLUSION

Today, good number of graphical password schemes are available but they have their advantages and limitations. In this study, we have conducted a comprehensive survey of existing password techniques in two main classifications to identify their strengths and weaknesses. From the study, we have proposed a graphical authentication system which is based on users day-to-day events to improve memorability of any chosen passwords on this system and reduce the users' memory load. The present study is limited to system implementation while our future action plan is to conduct the system comparative evaluation and users satisfaction survey.

7. ACKNOWLEDGMENT

The researchers would like to express their appreciation to Universiti Teknologi Malaysia, (UTM) for providing enabling environment for research.

8. REFRENCES

Adebola, O., N. Ithnin, M.Z. Jali and N. Akosu, 2013. Graphical password schemes design: Enhancing memorability features using autobiographical memories. J. Theoret. Applied Inform. Technol., 53: 124-130.

Almuairfi, S., P. Veeraraghavan and N. Chilamkurti, 2011. IPAS: Implicit password authentication system. Proceedings of the IEEE Workshops of International Conference on Advanced Information Networking and Applications, Mar. 23-25, IEEE Xplore Press, Biopolis, pp: 430-435. DOI: 10.1109/WAINA.2011.36

Biddle, R., S. Chiasson and P.C. Van Oorschot, 2012. Graphical passwords: Learning from the first twelve years. ACM Comput. Surveys. DOI: 10.1145/2333112.2333114

Bonneau, J., 2012. Guessing human-chosen secrets. University of Cambridge.

Chalkias, C., M. Petrakis, B. Psiloglou and M. Lianou, 2006. Modelling of light pollution in suburban areas using remotely sensed imagery and GIS. J. Environ. Manage., 79: 57-63. DOI: 10.1016/j.jenvman.2005.05.015

Chalkias, K., A. Alexiadis and G. Stephanides, 2006. A multi-grid graphical password scheme. Proceedings of the 6th International Conference on Artificial Intelligence and Digital Communications, (IDC' 06), Thessaloniki, Greece.

Chiasson, S., P.C. van Oorschot and R. Biddle, 2007. Graphical password authentication using cued click points. Proceedings of the 12th European Symposium on Research in Computer Security, Sept. 24-26, Springer Berlin Heidelberg, Dresden, Germany, pp: 359-374. DOI: 10.1007/978-3-540-74835-9_24

Davis, D., F. Monrose and M.K. Reiter, 2004. On user choice in graphical password schemes. Proceedings of the USENIX Security Symposium, (SS' 04).

Dhamija, R. and A. Perrig, 2000. Déjà Vu: A user study using images for authentication. Proceedings of the 9th conference on USENIX Security Symposium, (SS' 00), USA, pp: 4-4.

Dunphy, P. and J. Yan, 2007. Do background images improve "draw a secret' graphical passwords? Proceedings of the 14th ACM Conference on Computer and Communications Security, Oct. 29-Nov. 02, ACM, pp: 36-47. DOI: 10.1145/1315245.1315252

Forget, A., S. Chiasson and R. Biddle, 2010. Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Apr. 10-15, ACM New York, pp: 1107-1110. DOI: 10.1145/1753326.1753491

Hafiz, M.D., A.H. Abdullah, N. Ithnin and H.K. Mammi, 2008. Towards identifying usability and security features of graphical password in knowledge based authentication technique. Proceedings of the 2nd Asia International Conference on Modeling and Simulation, IEEE Xplore Press, Kuala Lumpur, pp: 396-403. DOI: 10.1109/AMS.2008.136

Jermyn, I., A. Mayer, F. Monrose, M.K. Reiter, ans A.D. Rubin, 1999. The design and analysis of graphical passwords. Proceedings of the 8th USENIX Security Symposium, (SS' 99).

Karnan, M., M. Akila and N. Krishnaraj, 2011. Biometric personal authentication using keystroke dynamics: A review. Applied Soft Comput., 11: 1565-1573. DOI: 10.1016/j.asoc.2010.08.003

Lashkari, A.H., S. Farmand, D. Zakaria, O. Bin and D. Saleh, 2009. Shoulder Surfing attack in graphical password authentication. Int. J. Comput. Sci. Inform. Security, 6: 145-154.

Lin, D., P. Dunphy, P. Olivier and J. Yan, 2007. Graphical passwords and qualitative spatial relations. Proceedings of the 3rd Symposium on Usable Privacy and Security, (UPS' 07).

Nali, D. and J. Thorpe, 2004. Analyzing user choice in graphical passwords. Carleton University.

Nielsen, G. and M. Vedel, 2009. Improving usability of passphrase authentication. MSc Thesis, Technical University of Denmark.

Owens, J. and J. Matthews, 2008. A study of passwords and methods used in brute-force SSH attacks. MS Thesis, Clarkson University.

Tao, H. and C. Adams, 2008. Pass-Go: A proposal to improve the usability of graphical passwords. Int. J. Netw. Security, 7: 273-292.

Thorpe, J. and P. Van Oorschot, 2004. Towards secure design choices for implementing graphical passwords. Proceedings of the 20th Annual Computer Security Applications Conference, (SAC' 04).

Tiwari, A., S. Sanyal, A. Abraham, S.J. Knapskog and S. Sanyal, 2011. A multi-factor security protocol for wireless payment-secure web authentication using mobile devices. Institute of Information Technology.

Tyagi, V.K., S.K. Chowdhary and N. Garg, 2011. Notice of Violation of IEEE Publication Principles Authentication using graphical password to upgrade security and memorability. Proceedings of the IEEE Recent Advances in Intelligent Computational Systems, Sept. 22-24, IEEE Xplore Press, Trivandrum, pp: 031-035. DOI: 10.1109/RAICS.2011.6069267

Vu, K.P.L., R.W. Proctor, A. Bhargav-Spantzel, B.L. Tai and J. Cook *et al*., 2007. Improving password security and memorability to protect personal and organizational information. Int. J. Human-Comput. Stud., 65: 744-757. DOI: 10.1016/j.ijhcs.2007.03.007

Wiedenbeck, S., J. Waters, J.C. Birget, A. Brodskiy and N. Memon, 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. Int. J. Human-Comput. Stud., 63: 102-127. DOI: 10.1016/j.ijhcs.2005.04.010

Zhang, J., X. Luo, S. Akkaladevi and J. Ziegelmayer, 2009. Improving multiple-password recall: An empirical study. Eur. J. Inform. Syst., 18: 165-176. DOI: 10.1057/ejis.2009.9

Zhao, H. and X. Li, 2007. S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. Proceedings of the 21st International Conference on. Advanced Information Networking and Applications Workshops, May 21-23, IEEE Xplore Press, Niagara Falls, Ont., pp: 467-472. DOI: 10.1109/AINAW.2007.317

Christopher, M., R. Lowson and H. Peck, 2004. Creating agile supply chains in the fashion industry. Int. J. Retail Distribut. Manage., 32: 367-376.