Journal of Theoretical and Applied Information Technology
10th July 2013. Vol. 53 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

GRAPHICAL PASSWORD SCHEMES DESIGN: ENHANCING MEMORABILITY FEATURES USING AUTOBIOGRAPHICAL MEMORIES

[1]OBASAN ADEBOLA, [2]NORAFIDA ITHNIN, [3]MOHD ZALISHAM JALI,[4]NICHOLAS AKOSU
[1,2&4] Universiti Teknologi Malaysia, Faculty of Computing,
81310 UTM, Skudai, Jorhor-Bahru, Malaysia
[3]Faculty of Science & Technology Universiti Sains Islam Malaysia,71800 Bandar Baru Nilai, Negeri Sembilan, Malaysia
Corresponding Author: Obasan Adebola O. Department of computer systems & Communnication, IASRG Lab, Faculty of Computing at University Technology Malaysia, 81310, Skudai ,Johor Bahru, Malaysia

ABSTRACT

Memorability and security of passwords are two distinct extremes that are difficult to achieve at the same time. These two important features are a major problem in conventional textual password systems. Text-based is a system where memorability is inversely proportional to security of passwords as such users choose weak texts as passwords to make it easy for themselves to remember at the expense of security. A weak password is easy to remember but provide little or no security because weak password is easy to break. To correct this flaw , graphical passwords are developed as an alternative to text-based passwords. However, a number of existing graphical schemes still have some drawbacks. The present study introduces a framework of a graphical password scheme using autobiographical memories to improve the memorabily of passwords. With this feature, user can write or draw two characters in each round of the grid cells for three rounds during the password creation and later use the corresponding cells in three rounds for authentication, without touching the grid system in order to prevent the password from being seen by any nearby observer and ultimately to resist against shoulder surfing

Keywords: *Autobiographical Memory, Shoulder Surfing, Graphical Passwords, Draw-Based Schemes*

1. INTRODUCTION

Information resource is a valuable and useful asset for both personal and corporate day to day life. Information is so valuable that it cannot be left unprotected from the reach of an intruder. The intruder is always ready to gain unauthorized access to an information system with the help of knowledge of some users' password and access the system of the original owner. It is therefore worthwhile to authenticate the user with what he knows to ensure that access is granted to the legitimate and the original user. To achieve the objective, login ID and password are issued to or generated by the user. Ordinarily without persuasion , users choose passwords that are weak and guessable being the most convenient way to ensure easy password creation and long-term memorability. These weak and guessable passwords include family name, first name , birthday, and phone number , and their predictable variants. This users' practice of choice of weak passwords opens information systems to a number of vulnerabilities. These include eavesdropping, dictionary attacks, shoulder surfing , offline and online guessing attacks. To secure password protected systems ,some website administrators inhibit some user-chosen passwords. For system to facilitate user choice of passwords and to resist these inadequacies, there are many alternatives . Graphical password systems are a alternative to text-based passwords.

Graphical password systems are made to leverage the ideal of image superiority effect concept, meaning that people have better memory images or pictures better than letters,

texts, and even sentences. This concept was established through the experiment conducted by Shepard [1] where it was found that human users were able to recognize 98.5% images accurately after 60mins delay , which was not possible with letters, texts, and sentences. The applications of this concept is what brought graphical passwords to the lime light. Graphical passwords employ images or patterns to achieve dependable user authentication via a mouse , stylus or other graphical devices. The simple reason why graphical passwords are more memorable than text-based passwords is picture superiority effect. Currently, there are a number of graphical password systems in different classifications using different cognitive activities for their operations [2]. First, there exist Locimetric graphical password systems where user select target points within a predetermined image in a specific order. Second, we equally have drawmetric passwords where the users have to draw a predetermine outline image on a touch screen grid. And thirdly, we have cognometric systems where the user needs to recognize a target object in a set of distractor objects or images. For all these schemes to function effectively, different memory features must be considered to improve memorability of user-generated passwords or passwords recollection using any of the schemes.

Therefore, memory is a fundamental requirement for password management and different means or features for improving memory should be considered important in authentication schemes development, because they could be tapped to improve password recollection [3]. These memory features include autobiographical memory, mnemonic strategies. Autobiographical memory consists of personal experiences and specific objects, people and events experienced at particular time and place recollected from an individual's life, and general knowledge and facts about the world [4] . While mnemonic strategies are hints of any kind that improves memorization of passwords [3]. Mnemonics helps us to associate the random or complex password to be recalled with a visual image, a sentence, or a word. Therefore , Mnemonic devices include; visual image, acrostic (or sentence), acronym, rhymes and alliteration, method of loci and chunking. They could be reliably used to improve password recollection. The work in this paper is organized as follows: we discussed related work in section 2, while in section 3 discussion is made on the proposed scheme, autobiographical memory is outlined in section 4 , while autobiographical memories graphical password design is discussed in section 5, and conclusion is made in section 6.

2. RELATED WORK

Graphical password is a secret entered to a computer system by human user with the help of graphical devices like mouse, stylus, or touch screen for the purpose of user authentication. The examples of these devices . Therefore, graphical password schemes are knowledge-based authentication systems and effective alternative to alphanumeric passwords where users create their passwords by selecting from images, in a specific order, presented in a graphical user interface [5] instead of use of text to log in. The development of graphical password schemes was born out of intention to increase the passwords usability with the help of pictures. Graphical passwords are of many kinds with different approaches. The first of all is called locimetric, they are graphical systems designed in which user create password by just clicking on different locations on a single image. These schemes are also called click-based or cued-recall graphical passwords. For authentication, he or she clicks on the predetermined areas of the locations [5] in a particular sequence. Examples of these scheme include PassPoints designed by [6] , Cued Click points and Persuasive cued Click-Points both are designed by [7].

Secondly, we have cognometric also called recognition-based systems, where the user needs to recognize and identify images which are part of his or her password images or target images in a set of distractor images or object. A popular example of this scheme is PassFaces (Real User Corporation,2004).

Thirdly, drawmetric also called recalled-based passwords where the users have to draw an image on a touch screen grid. For authentication, the user reproduce a drawing on the same grid. Example of these schemes include Draw-a-Secret and Pass-Go designed by [8] and [9] respectively. They both use user-defined drawings

on 2D grid as graphical passwords for the user authentication purpose. Since the security of any password depends on the length , giving any reasonable-length passwords in a 5x5 grid as in that of DAS , it was confirmed that the full password space of DAS scheme is more than that of the full textual passwords space with keyboard input characters. However, DAS and other schemes mentioned above are vulnerable to shoulder surfing and other limitations.

Shoulder- surfing problem is an attack in which the intruder can observe the passwords, PINs or other protected information by observing the owner or victim through his/her shoulder or other spying devices such as binoculars and video camera while the password is being used on the computer or at the terminal for authentication . The main aim of the intruder for this attack is to use the observed credentials for illicit transactions in order to impersonate the real owner (the victim) afterwards. The root cause of this drawback is due the fact that users enter their secrets directly to some poorly designed user interface in a way that is easy for intruder to gain knowledge of the secret via observation.

To surmount this problem during authentication, a number of shoulder-surfing resistant techniques were proposed as helpful solutions to protect the user's secret from being observed for illicit usage. To protect recall-based graphical password systems such Draw-A-Secret and Background Draw-A-Secret DAS from shoulder surfing, three techniques which include decoy Strokes defense, disappearing Strokes, and line Snaking were proposed [10]. These techniques are used during a login procedure as a means of distracting shoulder surfer away from capturing the correct password drawn by the user for security reason. Decoy Strokes defense technique allows user to draw many passwords of which only one is authentic user's password. In disappearing stroke defense, the user stroke is being removed from the screen after it has been drawn. The idea behind is to make it difficult for attacker to store the image to memory. While line Snaking technique is based on the disappearing stroke solution but was intended to leave the vital password information onscreen for an even shorter period. The onlooker is not given a chance to observe a complete user password onscreen [10]. Forget , et la. Proposed a gaze-based authentication system called Cued Gaze-Points (CGP) and designed to resist shoulder surfing problem. It is a cued-recall graphical password scheme using eye-gaze as an input mechanism [11] where users select points on a sequence of images with their eye-gaze instead of mouse-clicks. The main idea of the scheme is to make it difficult for onlooker see the login credential through mouse movement and clicking. Haichang et al. designed a recognition-based scheme inspired by DAS drawing input method and the association mnemonics in Story for sequence retrieval was proposed [12]. This scheme is an improvement of Story scheme and has a wanted usability for PDAs. In this scheme, to create a password, user chooses several images from the set as his/her pass-images which are connected mentally with a story to remember them correctly during authentication. To authenticate, user draws a curve across both pass-images and decoys in the right order. The drawing input trick along with the complementary measures, such as erasing the drawing trace, showing tainted images, and starting and ending with randomly designated images provide a good resistance to shoulder-surfing [12]. Another textual-graphical password scheme designed to provide resistance against Shoulder-surfing is S3PAS [13] . The acronym stands for Scalable Shoulder- Surfing Resistant Textual-Graphical Password Authentication Scheme . The scheme exists in three different variants and each serves different security environments.

To login, system displays login image containing set of characters with user's original pass-characters ,then he or she has two options to login. User can login by making some clicks inside the invisible pass-triangles or by typing textual character chosen from inside or on the border of the pass-triangle via keyboard instead of mouse [13]. The whole idea is that user neither clicks or types his original pass- characters but session pass-characters or session pass-clicks

which determines the session password of the user . The resulting user session password is completely different from the user's original password thereby making the password secure even if when an attacker is within authentication vicinity. Another scalable and flexible hybrid password authentication scheme based on shape and text was also proposed to resist against hidden-camera and shoulder-surfing problem of graphical password schemes [14]. The scheme is designed for computer and mobile devices to provide the advantages of both textual and graphical password systems to ensure better security. It uses shapes of strokes on the grid as the origin passwords and allows users to login with text passwords with the help of keyboard.

3. PROBLEMS OF GRID-BASED GRAPHICAL PASSWORD SYSTEMS.

The following gives a number of problems and limitations of the grid-based systems like DAS:

i.) It involves difficult method of authentication because user must draw his/her password in the same 2D grid coordinate and in the same sequence.

ii.) Identifying used cells for drawings whose strokes are too close to a grid-line may be difficult because it could hard to differentiate which cell was chosen by the user.

iii.) To identify a starting point for some drawings like oval shape figure can be hard.

iv.) They are highly vulnerable to guessing, hidden camera and shoulder surfing attack when used in public places.

v.) They have small effective password space because users tend to choose weak passwords thy can easily recall.

4. AUTOBIOGRAPHICAL MEMORY

Memory is simply ways we store and recall things we have sensed. Human memory plays a central and fundamental role in user authentication systems from when passwords are created to the time they are used for login. Human memory system consists of three memory stores. They include sensory store, which retains information very for a short while. The second is the short-term memory, it holds information for a very short period of time in a store of limited capacity. While the last one is long-term, which holds information over long periods of time or permanently [15] . The long-term memory can be sorted into two categories, namely, implicit and explicit memories. Implicit memory is a type of memory in which previous experiences aid in the performance of a task without conscious awareness of these previous experiences. Explicit memory also called autobiographical memory is recollection of memories that people have about personal events that were experienced at a specific moment in time [16] . It consists of personal experiences and specific objects, people and events experienced at particular time and place recollected from an individual's life, and general knowledge and facts about the world [4] . It deals with life experiences comprising specific events and personal facts related to oneself. This memory feature can be used as the basis for improving user authentication leveraging your own autobiographical data. Individual. The first study in this area focused on understanding and categorizing what kinds of everyday memories people could recall and the result was used to understand the relationship between various factors and memorability [4] .

5. AUTOBIOGRAPHICAL MEMORIES GRAPHICAL PASSWORD DESIGN

Proposed here is a grid based graphical password scheme whose design is based on the use autobiographical memories of the user to improve memorability of graphical passwords. It also employs 3-round process of authentication to improve security.

How the scheme works

Our proposed system works in three (3) main steps. The first 2 steps are used as registration process of the scheme as illustrated in Figure 1. While the last step is use for the scheme authentication as illustrated in Figure 2.

The system is a draw-based graphical password system with a background and it offers many advantages over the DAS in terms of security and memorability for the users. The operational framework of the design process will be discussed in two different stages , namely: registration and authentication as explained below:

a.) The first step in the user registration phase of this scheme is where the user types his or her user ID.

b.) If the user ID is a new one then he selects or picks a desirable background image for the grid. Then write down his secret character on the grid with any graphical device like mouse or stylus . Repeat the process for three times. After a successful registration, the registration details consists of image background grids , the user-choose character, user ID and password in asterisk.

c.) During the authentication phase, the user enters both user ID , if the user ID exists then the system displays three grids , each containing random digits on the chosen background images. User chooses corresponding digits on the image background where the characters were written during registration stage.

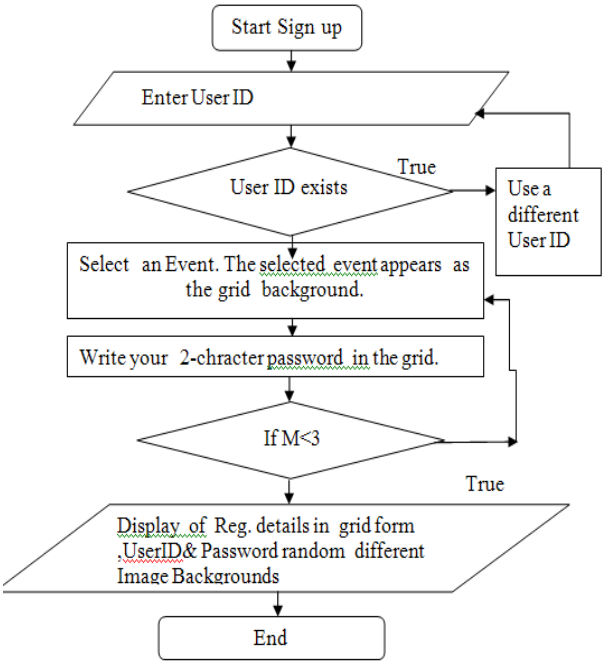

Figure 1 : Flowchart of Registration phase

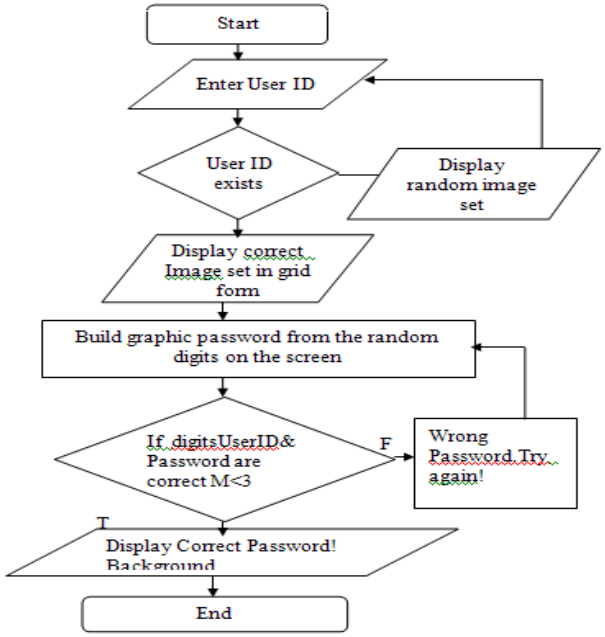

Figure 2 : Flowchart Of Authentication Phase

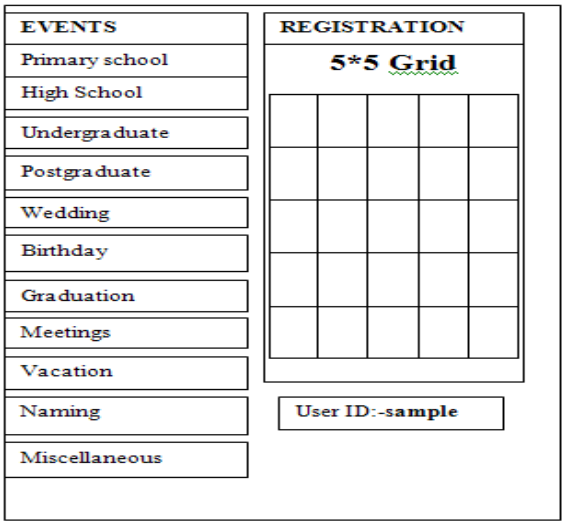

Figure 3 : Flowchart Of Password Authentication Phase

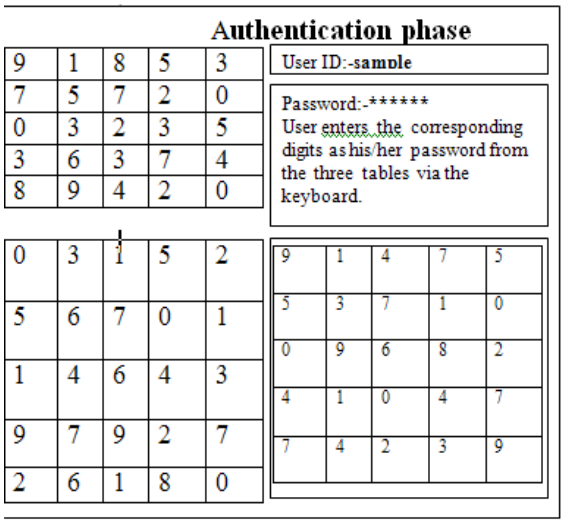

Figure 4 : Flowchart Of Password Authentication Phase

. CONCLUSION

There is a commonly known tradeoff between memorability and security of password authentication systems. Being that more secure passwords are less memorable. To redeem this flaw, a number of authentication methods and techniques has been put forward but memorability and security issues still remain as each limitations. These two factors influence the success of passwords. Many schemes are not memorable just because the required memory feature does not portray what people remember most in their design. In the light of this , we have proposed authentication system which is based on autobiographical memories of the users to improve memorability of graphical passwords and randomly generated digits are displayed on the screen for user to enter digits corresponding to the password via keyboard rather than graphical input devices like mouse and stylus in order to resist shoulder surfing attack. Currently we are working on the scheme implementation and performance analysis in order to address some important issues like memorability , security and even the user's factor of our scheme and they will be published soonest.

ACKNOWLEDGEMENT

The authors would like to express their appreciation to Universiti Teknologi Malaysia , (UTM) for providing conducive environment for research. Also, enormous support provided by the members of staff of faculty of computing is highly appreciated.

REFERENCES

[1]. Shepard, R.N., *Recognition memory for words, sentences, and pictures.* Journal of Verbal Learning and Verbal Behavior, 1967. **6**(1): p. 156-163.

[2]. De Angeli, A., et al., *Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems.* International Journal of Human-Computer Studies, 2005. **63**(1): p. 128-152.

[3]. Nelson, D. and K.-P.L. Vu, *Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords.* Computers in Human Behavior, 2010. **26**(4): p. 705-715.

[4]. Das, S., et al., *Evaluating the Use of Autobiographical Memory for Authentication.*
[5]. Blonder, G.E., *Graphical password*. 1996, Google Patents.
[6]. Wiedenbeck, S., et al., *PassPoints: Design and longitudinal evaluation of a graphical password system.* International Journal of Human-Computer Studies, 2005. **63**(1): p. 102-127.
[7]. Chiasson, S., *Usable authentication and click-based graphical passwords.* 2008, Carleton University.
[8]. Jermyn, I., et al. *The design and analysis of graphical passwords*. 1999: Washington DC.
[9]. Tao, H., *Pass-Go, a new graphical password scheme*. 2006, University of Ottawa.
[10]. Zakaria, N.H., et al. *Shoulder surfing defence for recall-based graphical passwords.* in *Proceedings of the Seventh Symposium on Usable Privacy and Security*. 2011: ACM.
[11]. Forget, A., S. Chiasson, and R. Biddle. *Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords*. in *Proceedings of the 28th international conference on Human factors in computing systems*. 2010: ACM.
[12]. Haichang, G., et al. *A new graphical password scheme resistant to shoulder-surfing*. in *International Conference on CyberWorlds*. 2010: Institute of Electrical and Electronics Engineers.
[13]. Zhao, H. and X. Li. *S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme*. in *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*. 2007: IEEE.
[14]. Zheng, Z., et al., *A Hybrid password authentication scheme based on shape and text.* Journal of Computers, 2010. **5**(5): p. 765-772.
[15]. Atkinson, R.C. and R.M. Shiffrin, *Human memory: A proposed system and its control processes.* The psychology of learning and motivation, 1968. **2**: p. 89-195.
[16]. Kristo, G., S.M. Janssen, and J.M. Murre, *Retention of autobiographical memories: An Internet-based diary study.* Memory, 2009. **17**(8): p. 816-829.