Journal of Physical Science and Innovation
ISSN: 2277-0119
Volume 9, No. 1, 2017

GRAPHICAL PASSWORDS AND METHODS FOR ENHANCED PASSWORD MEMORABILITY

Obasan Adebola, Abdulazeez & Sikiru, Patrick Owohunwa

Department of Computer Science, Kaduna Polytechnic
Department of Mathematics and Statistics
College of Science & Technology, Kaduna, Kaduna State, Nigeria.
Email: aolukay@yahoo.com, ysabdul94@yahoo.com, owohunwapatrick@yahoo.com

ABSTRACT

Corporate organizations are depending on Internet-enabled Information Technology to reach their target users is a common practice today. This development has made huge users to employ the same technology to satisfy their diverse needs. Consequently, computer and information security has become a critical from service provider viewpoint to achieve protection, confidentiality, integrity, and ensure reliable access to information resource when using computer systems. To achieve this, text-based password authentication has been widely used without flawlessness because remembering secure password chosen from mixture of random alphanumeric and non-alphanumeric characters is an everyday problem for all users because of individual memory limitation. Graphical password which works just by clicking with a mouse or stylus could be used for user authentication. In this paper, we highlight needs for study of password, how memory influences passwords, different methods for improving memorability of passwords and memorability to achieve the main objective of the study. Which is to design a graphical authentication system that uses three autobiographical events background images in draw-grid environment to reduce memory loads of password and to ultimately achieve better memorability and security of passwords. We also highlight memorability and security features of the proposed scheme.

Key words: Graphical passwords, Password Space, Authentication, Security, Memory, Memorability

INTRODUCTION

Currently, information systems are taking over all our day-to-day activities being it banking, accounting, and others. As such, they require some measures of control and protection to ensure reliability , integrity , and other security goals [1]. In order to achieve reasonable level of protection text-based passwords have been widely used for identification , authentication, and authorization 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 user authentication proves user's claimed identity as being right or wrong depending on username and corresponding password. On the other hand, authorization deals with the users' right to access resources ones they are authenticated. User authentication mechanism is part of security requirements which are often employed to secure internet and ensure the most needed protection of both the user and service provider. As a result of lack of natural safety in some communication channels , internet has been made to identify a number security challenges such as attempting to acquire information like usernames, passwords, credit card details by masquerading as a trustworthy entity in an electronic communication, and many other attacks.

Most of these problems are caused by weak user authentication which arose from weak choice of keyboard-based passwords consciously made by the users to enhance his or her memorability because users generally find it difficult or impossible to remember high-quality passwords that would guarantee security . In attempt to 'enjoy unethical' memorability, where users do not follow all the rules required of them for forming strong passwords. These rules include ; passwords must not relate to personal

information like name, birthday, even words found in a simply dictionary, password must have at least eight alphanumeric characters which should combination of upper and lower case letters with at least one digit ref. Mostly, they enjoy easy password to achieve cheap memorability at the expense of general security of the system. Therefore, user authentication system should be designed to provide two important features simultaneously, namely; usability and security. But in reality , one of these features is achieved while the other is ignored even though both are important and necessary. This problem is peculiar to text-based authentication systems because it requires human ability when needs arise.

As a result of these inadequacies in text passwords , alternative technologies such as public key cryptography , security token, biometric [2, 3] cognitive passwords and even hybrid of these authentication factors are gaining much attention to overcome problems in the text-based password authentication. Figure 1 shows the major authentication alternatives. However, the problem with these systems is that most of them are designed by the service providers to be cost effective scalable and secure , which sometimes creates difficulty and poor usability from the users' perspective.

Moreover, It is worthwhile to say that these alternative technologies do not provide solution to authentication problems without taking another cost. The reason is because each of them has one limitation or the other. Token could improve the level of security and protection but in the simplest vulnerability is should it lose, authentication could be more difficult if not totally impossible . Similarly, biometric technology has both his good and bad sides. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods, however, the database for storing of biometric identifiers is problematic when is compromised [4] .

Therefore, in an attempt to improve the limitation, another form of knowledge-based authentication called usable authentication which uses graphical password schemes was brought to lime light in 1999 [5] being the first study of its kind. They are potentially more memorable and secure than conventional text-based passwords because human users have the ability to easily recognize and recall images [4].

The main focus of this study is to improve user authentication in order in terms of memorability and security of efficient schemes that offer improved memorability and security, and the identification of some underlying design strategies to inform the design of other image-based authentication schemes. Today, a good number of usable authentication schemes like graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies supports such assumption [5]. A number of work had been done , which resulted into the existence and implementation of some graphical schemes with one limitation and other [6] [7]

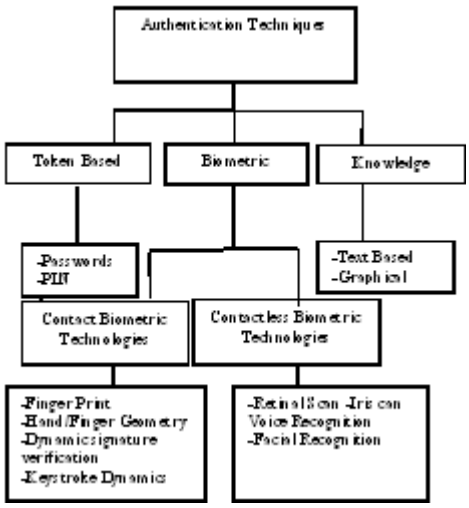

Figure 1: Classification of Authentication System

Graphical Password Schemes and Passwords Problems

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA). In this light, we will focus on our decisive efforts on this authentication alternative called graphical passwords where pictures are used as passwords instead of texts. The specific type graphical password for this study will be recognition and recall schemes. These schemes require users to click on different locations in a background image with the help of graphical devices such as mouse or sort keyboard to form the user's graphical password in the click or drawing sequence.

They have large password space and they are easy to use. However, there are many memorability and security problems with the existing graphical – based authentication schemes [8]. For the purpose of this study, considerable attention will be focused on cued-recall graphical password schemes called PassPoints [9] where passwords are sequence points anywhere on an image and draw-based schemes like DAS, BDAS where users make their passwords by drawing across the grid cells and they are not allowed to draw passwords across fussy boundaries [6]; [7]These schemes have a number of drawbacks [10] which include some security flaws like shoulder surfing or anonymous observation by nearby on looker , intersection attack, fuzzy boundaries problems and click-points are used in a relative sequence as user's password, which adversely affects memorability when the is long [6] ; [10]. User studies showed that the drawing sequences is hard to remember without committing illegal crossings made by tracing grid lines or crossing through cell corners [7].

Figure 2: An image used in the Passpoints System, Wiedenbeck, et al.

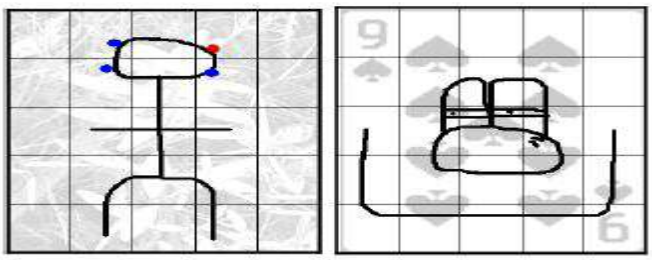

Figure 3: A sample of BDAS Algorithm

The scenario leading to the problem addressed in the current study as explained below in more details:

a.) In cued –recall schemes some locations of an image are more attractive and popular than the others and that users may tend to click on such locations as part of their passwords. An image with too many attractive locations could cause hotspot, and dictionary. Therefore, something must be done to avoid the attraction.

b.) The method does not have resistance to intersection and shoulder surfing attacks. A situation where malicious user or an attacker observes one login and derive enough information necessary for successful login process at later time without the knowledge of the correct owner of the password.

c.) Passwords are made from sequence of click- points anywhere on one single image instead of random choice of multiple background images to enhance the memorability of the passwords.

d.) Secure user-generated passwords are usually in a restricted long sequence of click-points which is difficult to remember. The large number sequence can divided into chunks or 3 units chosen click-points to enhance memorability of the passwords.

Needs for Study on Passwords

Internet enabled services require some level of security services like user authentication where users are expected to use their usernames and passwords to verify their identities. Ordinarily, users select passwords that are easy to remember and too weak to secure them because such passwords are highly predictable [11] . The need for this research was to use some memory features to ease the memorability of secure passwords for users. This Study is important and significant from both theoretical and practical perspectives. Therefore, the rationale and motivation for study of this type are as follows:

i) Passwords that are too difficult to remember may be forgotten and they are more likely to be written on paper by their owners. Writing down passwords, is a practice which some consider a security risk. Therefore, It is important to assist the users to use memorable and secure passwords to realize the full security for our day to day computer applications or internet enabled services.

ii) The fundamental expectation that users should remember their passwords without being assisted can only accommodate weak passwords, thus poses a security risk. Therefore, the process of choosing memorable and secure passwords must be made easy for users by providing visual aids that are not detrimental to the security of authentication systems.

iii) Imbalance between memorability and security is commonly found in knowledge-based authentication system and greatly impaired the effectiveness of such system [6] . Therefore, improved methods are needed.

iv) Incorrect submission of passwords is not only caused by memory failure but due to unintentional wrong use of input device against targets like fuzzy boundaries problem [6]. Thus, improved methods become imperative.

Memory and Its Influence on Passwords

Human memory is a topic that has been widely studies by many researchers because of the central role it plays in human existence and daily life endeavors [12] . Figure 5 illustrates the three main stages in formation and retrieval of passwords as in the case of memory. Password should be encoded, stored, and retrieved. Encoding allows password that is being formed from the outside world to reach our senses in the forms of physical stimuli. In this first stage, we must change the password information so that we may put the memory into the encoding process by paying enough attention while the password is being encoded. Storage is the second memory stage. This entails that we maintain password over periods of time. Finally the third stage is the recall of password that was stored. We must locate it and return it to our consciousness. Some recall attempts may be effortless due to use of weak passwords. Memory accuracy of the users is therefore necessary for login to be successful and this makes every user to memorize one or more passwords and recall them correctly at the time of login in order to gain access to secure network. Therefore, human memory plays a central responsibility in user authentication system. Figure 4, explains the way passwords are encoded and decoded at different stages of the memory.

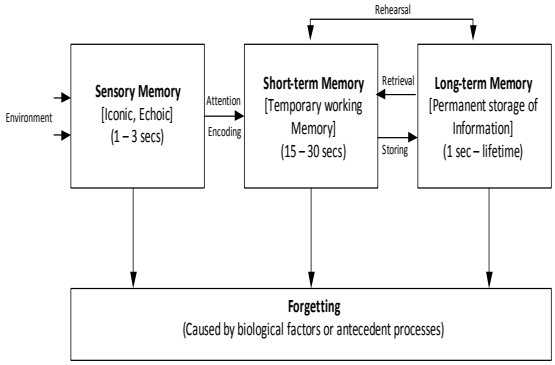

Figure 5: Multi-store model of memory

Human ability to recall useful information like password varies from one individual to another. The ability to recall password correctly and accurately can be partly determined by human memory effectiveness and partly by the design of password authentication system in use[13] . For the purpose of this research we only consider the effectiveness of the password authentication system design. This becomes necessary in order to focus on different means of improving password memorability without considering the good or bad memory effectiveness of the individual human users of the passwords.

Generally, average human user is expected to recall memorable passwords whenever and wherever is required for diverse applications. The study on memory in this form is necessary so that users would not find it difficult to generate secure passwords that are memorable at the same time without engaging in unsecure coping strategies while using passwords. The widely used practices include writing down password , choosing an easy-to-crack password and worse still, using the same password for more different application to ease password problems. Considering these limitations, it is worthwhile to examine or review different factors influencing human memory for generating memorable and secure passwords. It is therefore imperative to investigate various mean for enhancing human memory in order to ensure effective and efficient password systems to satisfy different users. To achieve this, many

studies have been conducted on memory improvement , especially on issues related to password authentication systems. They mostly focused on various memory tasks that relates to password accuracy , efficiency and strategies for achieving better performance of authentication system as summarized below[13]:

- Meaningful association of two or more distinct items in password strings can be used to facilitate its recall.
- It is widely recommended that recognition of familiar items facilitates recall.
- Recognition is better than pure recall and cued recall.
- In recognition-based, users are presented with a number of images and authentication is achieved by recognizing and identifying the images chosen during the registration process.
- In recall-based, users are required to reproduce image(s) that once created or used during the registration stage without any hints to influence or trigger the memory.
- In cued recall-based, users are required to reproduce image(s) that once created or used during the registration stage with the help of hints.
- Frequently used items are easier to remember than infrequently used one. When a password is frequently used by a user , recalling the password becomes almost automatic.
- Memory declines in performance with time or intervening events. The users' ability to retrieve items in memory depends on the number of items that must be retained otherwise known as memory load.
- People will ever recall some basic items on demand without delay. Some items are so basic that cannot be forgotten. But as such items increases, the number on forgotten items increases.
- Meaningful items are easy to recall but they weak to guess and therefore not secure.

Different Methods for Improving MEMORABILITY

There are many techniques and principles for improving memorability of passwords. They help users to recall their passwords accurately when needs arise. These measures include the following methods [12] :

Table 1: A summary of techniques for improving memorability

#	Techniques	Remark
1.	The generation effect	Self-generated passwords are better remembered.
2.	User's full attention	Each stage of memory require less than 30 seconds to encode new passwords. Users are required to pay absolute attention to ensure permanent storage.
3.	Use of many stimuli /Visual imagery	This could be colors, textures, pictures to enhance memory. All graphical passwords fulfill this simply because they are graphical in nature and they involve colors, textures, and even pictures.
4.	Relate password to prior knowledge	Something very known to you , like information on application, sites, place of work, friends and colleagues
5.	Use of random but logical Password	It is a good practice to use password that is suitable and applicable to your own words and not to someone else.

6.	Promote active manipulation	Increase the amount of practice of your chosen password .People remember information better if they practice using it more frequently.
7.	Use of mnemonic devices	Mnemonics are hints of any kind that improves memorization of passwords. They include: Acronym, Rhymes and alliteration, Method of loci, Peg Method, and Keyword mnemonic.
8.	Chunking	Is a process of breaking down a long and more mundane number or other types of information into smaller, more memorable chunks.
9.	Autobiographical memory	The memory of your own personal life history.

Proposed Password Scheme

The proposed method uses three boxes for authenticating a user. Our proposed system is adapted from the Passpoints algorithms and BDAS algorithms integrated with autobiographical memory and chunking. Autobiographical memory is the memory of your own personal life history and closely related to episodic memory [12, 14]. This type of memory plays an essential role in your unique sense of self. It is used in this design to provide necessary hints or cues and improve the memorability of the chosen passwords. While the chunking is adapted to allow user chose a secure and unpredictable passwords without constituting any memory load to the password owners. We call the system

Draw-Chunks EventGrid (DCEG) system because of the two memory features adopted in the its design [14].

Draw-chunks EventGrid system interfaces are presented in Figures 5 and 6 below. In draw-chunks (DCEG) system, the user performs the following activities in both registration and authentication stages. The interfaces for the phases are illustrated in Figures 5 and 6:

i.) Choses three autobiographical events of his choice to create your passwords.
ii.) The user draws his passwords in the three boxes one after the other.
iii.) The user enters his user name and click save button to complete registration phase.
iv.) To authenticate, the user enters his user name
v.) Then, use the onscreen keyboard to click those digits that correspond to you passwords across all the three boxes.
vi.) Click 'enter'.
vii.) Authentication is successful if the password matches with the user name or unsuccessful if mismatched

Memorability and Security Features

To incorporate memorability and security into both registration and authentication phases of this algorithm, a number of measures were considered. The use of pictures for authentication provides attackers an environment more vulnerable to attacks. Generally speaking, the graphical passwords all vulnerable to several types of attacks such as shoulder-surfing attacks, dictionary and spyware attacks. In our implementation, we used random digits to deceive an shoulder surfer. While the onscreen keyboard is intended to resist against spyware.

Autobiographical memory is the memory of user's personal life history [12, 15]. This feature is used in our implementation to provide a cue to trigger users' memory of their chosen passwords [16]. It is important to state that chunking helps both security and memorability of this algorithm. Simply because it allows users to choose complex passwords that are broken down into three meaningful chunks that influence memorability of secured passwords.

The users use drawing in the implementation of this system during registration process as illustrated in Figure 5 in order to provide an adequate number of possibilities of password combination to defeat dictionary and password guessing attacks. Draw-based schemes are characterized by strokes-counts drawn on three consecutive 5*5 grid system [17]. Figure 6 shows that users click instead of drawing during authentication process. It is also important to note that password space calculations of recognition-based graphical schemes often involve permutation since it involves random selection of images for choosing graphical. Given a set of size N images in a panel, the number a ways of choosing L passimages is called permutation denoted by P when the order of selection of L images out of total number images of N is important and the password space is defined by Equation 2.6 as follows:

$$S_L = {}^{N}_{L}P = \frac{N!}{(N-L)!} \quad (1)$$

Furthermore, the overall password space of a graphical password schemes where users choose an image more than once in to form a password when the order of passimages is important [18] can be calculated by Equation 1. This equation has been considered useful in this thesis to compute the overall password space of the proposed scheme since users are required to click a number of grid cells that match with their registered passwords from the available 25 cells.

It is importance to state that theoretical password space is a useful variable for obtaining password cracking times in order to determine how long a password can withstand guessing attack in terms of user attempt time and computer attempt time required by using Held and Bowers algorithm as stated in Equation 2 [19].

$$T = \left(\frac{S_L}{2}\right) * I * \left(\frac{1}{MIPS}\right) \quad (2)$$

Where:

T = Amount of time in seconds required to crack the password

S_L = Password space size

I= Number of instructions in the cracking algorithm

MIPS= Machine speed of the machine executing the algorithm

Figure 5.: DCEG Registration phase interface

Figure 6: DCEG Authentication phase interface

CONCLUSION

The story of password being lost , forgotten, sniffed, or even completely forged is not new in our day- to- day applications of computer and communication systems. It is not easy for human users to securely store high-quality cryptographic keys because of inability to remember such data unlike weak text-passwords which are often chosen by users as a coping strategy to remember and unfortunately such passwords are easy for intruders to crack. To develop and implement an enhanced authentication algorithm, the memorability and security features of the recognition and recall-based approach were tapped. To further improve the memorability rate of the scheme, autobiographical memory and chunking techniques were implemented in the scheme. The registration phase was designed similar to BDAS recall-based scheme in which users drew their passwords across the grid cells. While the recognition phase was designed similar to Passpoints recognition-based scheme in which users click the digits in the onscreen keyboard based the combination of digits that matched with their passwords. The fuzzy boundaries problem was also solved by onscreen keyboard because users would not need to draw during authentication phase. The study is expected to complement the better understanding of graphical password

authentication and computer network security. The same study was conducted in such a manner to provide a better approach in designing more effective password authentication system. As such, the study should be beneficial to both researchers and IT practitioners.

ACKNOWLEDGMENT

The authors would like to express their appreciation to Kaduna Polytechnic, (KPT) for providing conducive environment for research.

REFRENCES

1. ITHNIN, N. and C.S. WENG, *MEMORABILITY FEATURES OF DRAW-BASED GRAPHICAL PASSWORDS.* Journal of Theoretical & Applied Information Technology, 2013. **53**(1).
2. Maltoni, D., et al., *Handbook of fingerprint recognition*. 2009: springer.
3. Gilhooly, K., *Biometrics: Getting back to business.* Computerworld, May, 2005. **9**.
4. Suo, X., Y. Zhu, and G.S. Owen. *Graphical passwords: A survey*. in *Computer Security Applications Conference, 21st Annual*. 2005. IEEE.
5. Jermyn, I., et al. *The design and analysis of graphical passwords*. in *Proceedings of the 8th USENIX Security Symposium*. 1999. Washington DC.
6. Dunphy, P. and J. Yan. *Do background images improve Draw a Secret graphical passwords?* in *Proceedings of the 14th ACM conference on Computer and communications security*. 2007. ACM.
7. Chiang, H.-Y. and S. Chiasson. *Improving user authentication on mobile devices: a touchscreen graphical password*. in *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*. 2013. ACM.
8. al-Khateeb, H., C. Maple, and M. Conrad, *Hybrid pass: authentication mechanism for web applications–both secure and user-friendly.* 2009.

9. 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.
10. Jali, M.Z., *A Study of Graphical Alternatives for User Authentication.* 2011.
11. al-Khateeb, H., *Security and usability in click-based authentication systems.* 2011.
12. 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.
13. Vu, K.-P.L., et al., *Improving password security and memorability to protect personal and organizational information.* International Journal of Human-Computer Studies, 2007. **65**(8): p. 744-757.
14. Obasan Adebola, N.I., Mohd Zalisham Jali, Nicholas Akosu *Graphical Password Scheme Design: Enhancing Memorability Features Using Autobiographical Memories* Journal of Theoretical and Applied Information Technology, 2013. **53**(1): p. 7.
15. Thompson, C.P., et al., *Autobiographical memory: Remembering what and remembering when.* 2013: Psychology Press.
16. Isola, P., et al. *What makes an image memorable?* in *Computer Vision and Pattern Recognition (CVPR), 2011 IEEE Conference on.* 2011. IEEE.
17. Davis, D., F. Monrose, and M.K. Reiter. *On User Choice in Graphical Password Schemes.* in *USENIX Security Symposium.* 2004.
18. Meng, Y. Designing click-draw based graphical password scheme for better authentication. In Proceedings of IEEE 7th International Conference on Networking, Architecture and storage (NSA). June 8-10, 2012. China, 1-10.
19. Held, J. S. and J. Bowers (2001). Securing e-business applications and communications, CRC Press.

Reference to this paper should be made as follows: Obasan Adebola, Abdulazeez & Sikiru, Patrick Owohunwa. (2017), Graphical Passwords and Methods for Enhanced Password Memorability. *J. of Physical Science and Innovation, Vol. 9, No. 1, Pp. 25 – 43*