A Secure Usability Design System for User Authentication

Ayannuga Olanrewaju O.[†], Folorunso Olusegun[††], Akinwale Adio T.[††]and Asiribo E. O.[†††],

[†]Department of Computer Technology, Yaba College of Technology, Yaba, Lagos, Nigeria.
[††]Department of Computer Science, University of Agriculture Abeokuta, Nigeria
[†††]Department of Statistics University of Agriculture Abeokuta, Nigeria

Summary
The term usable authentication is been brought about as a result of issues surrounding user memorabiilty. Computer users find it less easy to memorize plain text password compared to images or graphics. Researchers have over the years presented several authentication schemes in an effort to provide users with a usable and yet secure authentication system. Authentication and usability are two important terms that to a large extent determines how good a security system is. Secure systems are often needed in many organizations to keep privacy, ensure data safety, among many others. Though it is a necessity for such systems to be very secure but one thing often neglected by most developers is the user. When a system is too secure that it often leads to circumventing of the system by the users, then such a system is not usable. This paper takes a close look at how usability and authentication can be balanced with the use of graphical passwords by presenting an authentication system that combines the use of text based password and graphics based password. The combined strengths of these schemes present computer users with a secure yet usable authentication scheme.

Keywords
Authentication, Graphical Password, Security, Text Password and Usability.

1. Introduction

With the reduction in the cost of acquiring computer system and huge advancement in the use of computer in many applications such as data transfer, sharing data, login to E-mail or Internet, there is increase in the number of users, which implies increase in data stored in electronic database. This poses a challenging task for system and network administrator to determine user authentication. Authentication has been the catalyst for business organization in information protection and security. In [21], it was stated that Authentication is the process of determining whether a user should be allowed access to a particular system or resource. In [15] it was opined that Authentication is the process of verifying the identity of a certain person. User Authentication involves issues of both usability and security; too often one or the other is ignored even when it is clear that both are important and necessary. To be effective as an authentication mechanism, passwords must simultaneously satisfy two conflicting requirements: they must be difficult to compromise, yet easy to remember. This challenge underscores the importance of considering user behavior when developing security solutions. If users are allowed to create their own passwords, they tend to use common words, names, dates, or other personal information that can be easily remembered [2].

2. Authentication

Authenticating is the process of verifying the identity of a certain person. This has been used for many different purposes throughout history e.g., scouts and other messengers needed to authenticate themselves to city guards and sentries in the past before they were given access to different areas [15].

In the modern electronically wired information society, authentication has gained an even more important role, where user authentication is used to grant access control for many computer systems (UNIX, Linux and Windows). User authentication on these operating systems is usually based on password authentication. The user will hold a username and a password that also is known to the operating system. The authentication process is successful and access is granted if the username and password entered matches the stored values in the operating system. Password user authentication is the most common type of authentication used to ensure system or document protection and it is therefore important to use a secure authentication scheme for these purposes [17]. Password authentication can also be denoted as shared secret authentication, because the user that needs to be authenticated shares a common secret with the operating system.

Manuscript received April 5, 2011
Manuscript revised April 20, 2011

Figure 1 illustrates different types of authentication, which is commonly used in the modern information society.

(a) A smartcard can be used in a token based authentication system.

(b) The lock expresses an authentication system, where the user needs a key to authenticate.

(c) The login box is a standard secret based authentication system from Windows and

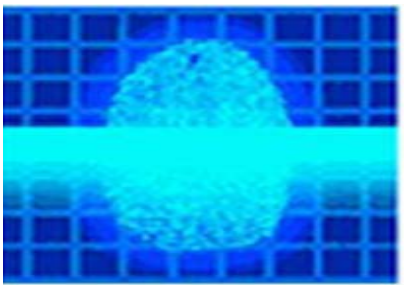
(d) The finger scan expresses a form of biometrics that authenticates the user on the biological characteristics.

(e)

(a) Smart card

(b) Lock

(c) Login box



(d) Finger scan

Figure 1: Different authentication method

In medieval times scouts could authenticate themselves by the use of seals or similar tokens, but it could also be done through passwords that helped the authorities distinguish foreign people from local citizens [15]. Today we normally use pin codes, passwords, passports, keys, smartcards or other things to authenticate for different purposes, and sometimes a combination of several of these things is required for a specific authentication system. It is important to provide strong security for authentication systems. The harder it is for an attacker to gain access the better the security of the system is.

Authentication is usually said to be based on different principles [3]. It is something you have (ownership factor), know (knowledge factor), do or are (inherence factor) as illustrated in figure 1. In [3] highlighted three different principles (something the user knows, something the user has or something the user is). Each of these attributes illustrates different requirements a user has to fulfill if it should be possible to authenticate against a certain authentication system. Figure 2 shows the four different principles used for authentication. The description of figure two is as follows.

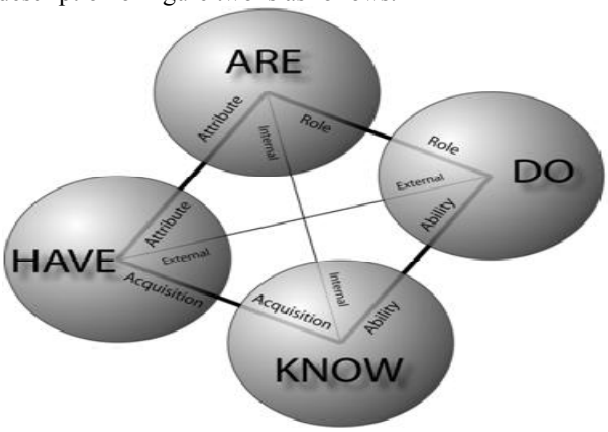


Figure 2: The 4 different principles used for authentication

Are: If you should authenticate yourself by proving that you are someone the most common thing is to use biometrics. This could be fingerprints, voice recognition, retina scan or other things, which proves the identity of the person. Things like fingerprints and retinas are considered unique, and thereby an attacker would have to obtain a copy of the required biometrics to be granted access to the system.

Have: This kind of authentication requires something you have. This could for example be some kind of a smartcard that identifies you or a normal key required to open up a door. These things belong to the owner, which means that it provides some kind of authentication for the user. A token is usually embedded with some kind of unique information, which is needed if it should be possible for an attacker to duplicate the token.
An authentication token that belongs to a person like a smartcard or a key is easily stolen by someone who wants to obtain the person's identities. This is a security issue in using a physical token that can be stolen by a thief or some other person that wants the permissions which the authentication token grants. To provide a better security solution the authentication process should include both a token and something the person knows like a password.
Passports, driver's licenses or health insurance cards are other things that can prove the identity of a certain person. It could also be assumed that a person should authenticate himself by proving he has a specific employment or belongs to a university. This could be done with different kind of identity cards issued by the authority to which the person belongs. Authenticating by using something you have might involve severe security risks because of the possibility to make false identity cards and authenticate as someone else.

Know: By using this form of authentication the user reveals something he or she knows. This is most likely a password or a passphrase, which has been used for thousands of years when people authenticate themselves for different purposes.
UNIX and Windows do also use this kind of knowledge authentication for their traditional login system. It is not easy to obtain a password from another person, but it might be achieved by using social engineering, keyloggers, key sniffers or looking over someone's shoulder.

Do: With this form of authentication it is something that a person does. This could for example be a signature. A person signs a document or anything else to prove that he is the right person. A signature could also be duplicated by another person. It is difficult to make a perfect duplicate, but it might be possible to commit fraud by making a signature that looks like the real one. In [7], it was stated that trained document examiners can have a false acceptance rate of around 25% and untrained personal like bank employees will accept almost 100% in practice. This is a security issue for something you do to prove your identity.
All of these authentication types define some examples of what a person could do to authenticate him and prove that he is the person he claims to be. Signatures and personal identity cards could be duplicated and tokens could be stolen. This means that the security of the authentication provided by these methods is rather weak on its own. This could be increased by combining the authentication types by using a multifactor authentication system. If a person both uses something, which is known and a token, then the security is increased by a great margin. An attacker would need to obtain the information needed for both authentication types and thereby the security of the authentication system increases. This could also be described as a layered authentication approach, where several layers of authentication strengthen the overall security of the system.
In [16] Renaud came up with his model which state that, authentication process can be described as three phases: identification, authentication, and authorization. Users must first make some claim of their identity, provide evidence to substantiate this claim, and if successfully authenticated by the system, access rights are granted to the user.

We classify authentication mechanisms according to the following five principles, primarily based on [16]:

1. **Something you know (recall):** A secret is shared between the user and the system. Users must recall and correctly enter their secret to authenticate themselves. Anyone who knows or guesses the secret will also be able to authenticate as the original user. Examples include passwords and PINs (Personal Identification Numbers).

2. **Something you recognize (recognition):** The user and the system share a secret. The system provides cues and the user must correctly recognize the secret. Anyone able to recognize the secret will be able to authenticate as the original user. Graphical passwords where users must recognize pre-selected images from a set of decoys fall into this category. Cued recall systems combine recall and recognition. Users must recognize the cue presented by the system and then use this cue to recall the secret shared with the system.

3. **Something you are (static biometrics):** Biometrics measures some unique physical characteristic of the user. These are more difficult to forge than the first two categories but introduce additional concerns. They may require specialized equipment, are difficult or impossible to change if compromised, and have potential privacy implications (e.g., they may make it difficult to create different identities for various purposes, and they enable organizations to cross-reference information about a user). Static biometrics includes fingerprint, iris, and facial scans, among others.

4. **Something you do (behavioral biometrics):** Some unique behavioral characteristic of the user can also be measured. Users authenticate by repeating the required action. Examples include handwritten signatures and keystroke dynamics.

5. **Something you have (tokens):** Users must carry a token to be presented for authentication. Anyone who gains access to the token will be able to authenticate as the original user. These are often combined with a PIN or password to offer some protection in case the token is lost or stolen. A smart card, i.e., a card with embedded microprocessor chip, is an example of a token used for authentication.

3. Graphical Passwords

For over a century, psychology studies have recognized the human brain's superior memory for recognizing and recalling visual information as opposed to verbal or textual information [11]; [12]; [13]; [18]. The most widely accepted theory explaining this difference is the “dual-coding theory" [14], suggesting that verbal and non-verbal memory (i.e., word-based or image-based) are processed and represented differently in the mind. Images are mentally represented in way that retains the perceptual features being observed and are assigned perceived meaning based on what is being directly observed. Text is a form of knowledge representation. Text is represented symbolically, where symbols are given arbitrary meaning that describes the object represented by the text, as opposed to perceived meaning. For example, `X' may represent the Roman numeral 10 or the multiplication symbol; the exact meaning is assigned based on some deeper concept. Furthermore, images may be encoded twice, perceptually and symbolically, if meaning is assigned to the image.

Graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on the user, more secure (e.g., longer or more complex) passwords can be produced and users will not resort to unsafe practices in order to cope [9]; [6]. Graphical passwords can be categorized into Pure Recall, Cued Recall and Recognition.

3.1 Pure Recall

Graphical passwords requiring pure recall are most similar to text passwords because users must remember their password and reproduce it without any cues from the system. This is a difficult memory task [5] and users sometimes devise ways of using the interface as a cue even though it is not intended as such. For example, we have evidence that users often include the name of the system as part of their text passwords [4].

3.2 Cued-recall

In cued-recall systems, the system provides a cue to help trigger the user's memory of the password (or portion thereof). This feature is intended to reduce the memory load on users and is an easier memory recall task than pure recall. [20] explain that items in human memory may be available but not accessible for retrieval. Their results showed that previously inaccessible information in a pure recall situation can be retrieved with the aid of a retrieval cue. Ideally, the cue in an authentication system will be helpful only to legitimate users and not to attackers trying to crack a given password.

Several of the cued-recall graphical password schemes surveyed require that users remember specific details within the images (or 3D environment). This is a different memory task than simply recognizing the image as a whole. In [8], it showed that people also retain accurate, detailed, visual memories of objects to which they previously attended in visual scenes; this suggests that users may be able to accurately remember specific parts of an image as their password if they initially focused on them. We now provide a survey of graphical password systems that employ cued-recall to facilitate password memory.

3.3 Recognition

Several theories exist to explain the difference between recognition and recall memory, based on whether these are two unique processes or whether they are similar and differ only in their retrieval difficulty [1]. It is generally accepted, however, that recognition is an easier memory task than recall [10]. In recognition-based graphical password systems, users typically memorize a portfolio of images during password creation and then must recognize their images from among decoys to log in. Humans have exceptional ability to recognize images previously seen, even if those images were viewed very brief [18].

4. System Model and Design

This section describes the architecture and design of the proposed system. It presents the design requirements, tools as well as the architecture of the proposed system. Codes are written in PHP using MySql as the database as well as MySql3.23 hashes for the encryption.

4.1 Design requirement analysis

The proposed security system is designed using PHP and MySQL as the database. Users now have the ability to create both passwords as well as pass-images at sign-in. The proposed system presents the user with the following screen:

Figure 3: Application homepage

For new users the 'new user' option will be the choice to be made. When a user want to create an account, certain information should be known prior to the commencement of the process; the user must be able to identify three images in a sequence as well as memorize three passwords.

The first stage is to supply a user name. if the name already exist, then another has to be entered.

Figure 4: Account creation page

After successfully creating the username, the first pass image as well as password will be required in sequence as follows:

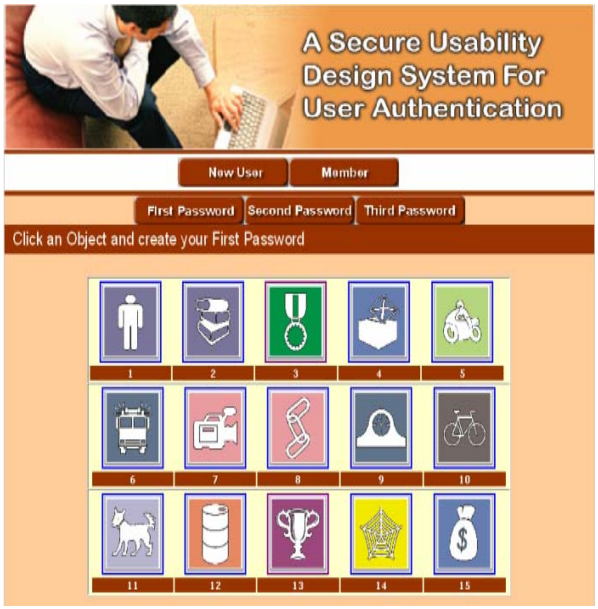


Figure 5: Image selection page

After choosing the first image, user is asked to supply a password of at least six characters in length as well as the username.

Figure 6: Login page

This process is repeated two more times with new sets of images and user is required to click just one from each set as well as supply a password.

For existing members to login to the system, all they need do is click on 'member', supply username and then supply the pass-images and passwords in the sequence for which the created the account.

4.2 Pseudocode of The Proposed System

Account creation phase

1. Click new user
2. Supply username
3. For n = 1 to 3
   Select pass-Image (one of fifteen)
   Enter supplied username
   Supply image associated password
4. End for
5. Echo successful account creation
6. End

Login process

1. Click member
2. Supply username
3. For n = 1 to 3
   Select pass-Image (one of fifteen)
   Supply image associated password
4. End for
5. Open the system into user environment
6. End

5. Definitions

Definition 1: User Account Setup

Let (U1, U2…, Un) be set of users in computer system C. Every user input username (N). Let (N) be an input in the system C such that $\forall$ S $\in$ U. U represents the user of the system.

Definition 2: Users Authentication

Let (U1, U2..., Un) be set of users in computer system C. Every username is bonded with sets of images. Let (I1, I2, I3) be three associated pass-Images to Ui where i is a positive integer. Ii indicates one pass-Image which is tied to a password. Let (P1, P2, P3) be set of password associated with (I1, I2, I3) such that Ui(I1, I2, I3) and Ii(Pi). For every authentication we have Un(Ii(Pi), Ii+1(Pi+1), Ii+2(Pi+2)) where i = 1 and n is a positive integer.

Note, length of username and passwords cannot be less than six characters and not more than twenty characters. Efficiency of the designed system is measured on a scale of ten based on the mathematical representation for the designed system. The efficiency scale is given below.

Classification	Efficiency levels (E_L)
Extremely efficient (very difficult to breach with average usability support)	0.00 - 3.50
Adequately efficient (sufficient security to hinder security breach with above average usability support)	3.51 – 7.00
Balanced efficiency (average security provision with average usability support)	7.01 – 10.0

Definition 3: Mathematical representation for the designed system

Let U_L be the length of username.

P_{SL} be the sum of the length of P1, P2 and P3

I_t is the total number of images per set

I_s is the number of images to select per set

N_s is the number of image set

T is the estimated average login time

$I_{SC} = ({}^{It}C_{Is})^{Ns}$ which is the image selection constant $({}^{15}C_1)^3 = 3.375 * 10^3$

$E_L = I_{SC} / T(P_{SL} + U_L)$ is **efficiency level** of the designed system.

Note: $6 \leq P_{SL} \leq 20$; $6 \leq U_L \leq 20$.

6. Conclusion

The goal of this research was to design a feasible solution based both graphics and text to improve the level of usability yet strengthens security of authentication systems. This work has presented a system that has leveled a balance between security and usability. The designed system has the combined capability of a very secure system as well as a usable authentication system. With several improvements on user authentication that has been proffered by researchers in recent years, graphical passwords scheme stands out as it is a convenient means of enhancing usability. The designed system uses graphical password to enhance its usability as well as to enhance its security. With the application of encryption to the text in the designed system, the systems security is strengthened which makes it difficult to compromise.

The designed system also worked on the strength of text length as the minimum number of characters permitted for both username and passwords is six characters. With the length of the username and passwords all being six characters, the systems efficiency level of 9.38 which is of balanced efficiency. In other words, the worst case scenario in the designed system yields a balanced efficiency. The best the designed system can give is 1.41 which indicates extreme efficiency. That result is possible if the length of the username and passwords are twenty. One can conclude by saying that, despite the improved usability with the use of images and the improved security with the use of encryption, the system efficiency of the system get better with a considerably long password and username.

References

[1] Anderson J. and Bower G. March 1972. Recognition and retrieval processes in free recall. Psychological Review, 79(2):97.

[2] Brown, Alan s.; et al, 2004. “Generating and remembering passwords” Applied cognitive psychology 18(6): 641-651

[3] Carlton F. Carlton, John W. Taylor, and John L. Wyszfynski. October 1988. Alternative authentication techniques. In Proceedings, 11th National Computer Security Conference, pages 333{338, Baltimore, MD, U.S.A..

[4] Chiasson S, Forget A., Biddle R., and van Oorschot P. September 2008. Influencing users towards better passwords: Persuasive Cued Click-Points. In Human Computer Interaction (HCI), The British Computer Society.

[5] Craik F. and McDowd J. July 1987. Age differences in recall and recognition. Journal of Experimental Psychology: Learning, Memory, and Cognition, 13(3):474{479.

[6] F. Monrose, M. Reiter, August 2005. "Graphcal password"

[7] Herbst N. M and C. N. Liu. 1977. Automatic signature veri_cation based on accelerometry. Technical report, IBM J. Research Development.

[8] Hollingworth A and Henderson J. 2002. Accurate visual memory for previously attended objects in natural scenes. Journal of Experimental Psychology: Human Perception and Performance, 28(1):113{136.

[9] Jermyn I., Mayer A., Monrose F., Reiter M., and Rubin A. August 1999. The design and analysis of graphical passwords. In 8th USENIX Security Symposium.

[10] Kintsch W. 1970. Models for free recall and recognition. In D. Norman, editor, Models of human memory, chapter Models for free recall and recognition. Academic Press: New York.

[11] Kirkpatrick B. 1894. An experimental study of memory. Psychological Review, 1:602{609.

[12] Madigan S. 1983. Chapter 3: Picture memory. In J. Yuille, editor, Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio, chapter 3. Picture Memory, pages 65{89. Lawrence Erlbaum Associates,.

[13] Paivio A., Rogers T., and Smythe P. 1968. Why are pictures easier to recall than words? Psychonomic Science, 11(4):137{138.

[14] Paivio A. 2006. Mind and its evolution: a dual coding theoretical approach. Lawrence Erlbaum: Mahwah, N.J..
[15] Richard E. Smith. October 2001. Authentication: From Passwords to Public Keys, chapter 2-3,6, pages 39{101, 155{192. Addison-Wesley Professional.
[16] Renaud K. 2005. Evaluating authentication mechanisms. In L. Cranor and S. Garffinkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6, pages 103{128. O'Reilly Media.
[17] Schneier Bruce. 1996. Applied Cryptography, chapter 8, pages 169{188. John Wiley & Sons, Inc.
[18] Shepard R. N. 1967. Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior, pages 156–163.
[19] Standing L., Conezio J., and Haber R. 1970. Perception and memory for pictures: Single-trial learning of 2500 visual stimuli. Psychonomic Science, 19(2):7374.
[20] Tulving E. and Pearlstone Z. 1966. Availability versus accessibility of information in memory for words. Journal of Verbal Learning and Verbal Behavior, 5:381{391.
[21] Wiedenbeck S., Waters J., Birget J, Brodskiy A., and Memon N. July 2005. Authentication using graphical passwords: Basic results. In 11th International Conference on Human-Computer Interaction (HCI International)