IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 6 (May. - Jun. 2013), PP 14-20
www.iosrjournals.org

A Study of Various Graphical Passwords Authentication Schemes Using Ai Hans Peter Wickelgren Approach

Pavan Gujjar Panduranga Rao[1] , Dr.G.Lavanya Devi[2] , Dr.P.Srinivasa Rao[3]
[1]Research Scholar, Department of Computer Science and System Engineering, Andhra University,
. [2,3]Professor,Department of Computer Science and System Engineering, Andhra University, Vishakhapatnam, Andhra Pradesh, India

Abstract: *Using AI Hans peter Wickelgren applying the usage of text-based passwords is common authentication system in any Application. This conventional authentication scheme faces some kind of limitations and drawbacks with usability and crypto-graphical security issues that bring troubles to users. For example, user tends to pick passwords that can be easily guessed. On the contrary, if a password is hard to guess, then it is often hard to remember. An alternative system is required to overcome these problems. To deal with these drawbacks, authentication scheme that use photo ,image, or set of pattern as password is proposed using knowledge Recall-Based System(KRBS).Graphical passwords consist of clicking or dragging activities on the pictures rather than typing textual characters, might be the option to overcome the problems that arise from the text-based passwords authentication system. In this paper, a comprehensive Artificial Intelligence(AI) study of the existing graphical password schemes is performed. The graphical password authentication systems are categorized into two AI approach types: An approach on recognition-based System (RBS) and second approach on Recall-based system (RCBS). We discuss adequately the strengths and limitations of each method in terms of usability and security aspects .*

Keywords- *Graphical Passwords using Hans peter Wickelgren, Recognition-Based Graphical User Authentication, Recall-Based Graphical User Authentication, Pure Recall-Based Authentication, Knowledge Recall-Based Authentication System, Usability, Security , Artificial Intelligence(AI) ,Knowledge-Based Development Systems(KBDS).*

I. Introduction

Many Web sites need authentication schemes to distinguish human from non-human users or to control distribution of content to select groups. However, today's Web access control mechanisms remain fairly cumbersome; administrators must maintain access control lists and user accounts, and users must remember and manage a large collection of graphical passwords. An authentication mechanism known as CAPTCHAs (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part") has gained popularity for distinguishing humans from non-human .Authentication is a process by which a system verifies the identity of a user .It is a process of determining whether a particular individual or a device should be allowed to access a system or an application or merely an object running in a device[14]. Authentication deals with the security as an act of showing the belongings to its owner only. Also, adequate authentication is the initial step of defense for protecting any resource. Various user authentication schemes are available these days. But out of these entire how many are truly secure? To answer it lets go through the back-ground of graphical passwords using AI approach . We deal with graphical passwords because graphical password schemes act as a possible alternative to text-based schemes which are proposed mainly by the fact that humans can remember pictures better than text [10]. Pictures are generally easier to be remembered or recognized than text, especially photo patterns. Graphical passwords is harder to guess or broken by brute force and digital marking . If the number of possible image patterns is sufficiently large, the possible password space of a graphical pass-word scheme may exceed that of text-based schemes and thus most probably offer improved security against hyperlink-text attacks. The use of graphical password methods is gaining awareness because of these advantages. Graphical passwords were originally described by Blonder [3]. In his description, an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated.

Two way Classification : Graphical Password Techniques

In general, the graphical password techniques can be classified into two categories: recognition-based and recall-based graphical techniques using AI technique.

Recognition Based System

Using recognition-based techniques, a user is presented with a set of image pattern and the user passes the authentication by recognizing and identifying the image pattern he or she selected during the registration stage in the system. There are many graphical password authentication schemes in knowledge Base which designed by using recognition-based techniques. They are discussed below. Jensen et al. [4] proposed a graphical password scheme based on "image or picture password" designed especially for mobile devices such as PDAs. Because mobile devices use PIN-based (Personal Identification Number) authentication, since they do not employ a standard QWERTY keyboard for conveniently entering text-based passwords. However, PINs provide a small password space size, which is vulnerable to attacks. Here, throughout the password creation, the user has to select the theme first (e.g. simple image pattern in contradictory with pixel patterns namely sea and shore, cat and dog and etc) which consists of thumbnail photo pattern. The user then selects and registers a sequence of the selected thumbnail photo to form a password (Fig. 1). The user needs to recognize and identify the previously seen photos and touch it in the correct sequence using a tablet-stylus type of graphical device in order to be authenticated. However, as the numbers of thumbnail photos are limited only to 30, the size of the password space is considered small. A numerical value is assigned for each thumbnail photo and the sequence of selection will produce a numerical password which may be programmed as even. This numerical password is shorter than the length of textual password. To over-come this problem a user can select one or two thumbnail photos as one single action in order to create and enlarge the size of the password space. However, this will make the understandability (AI) of the created password become more complex and difficult.

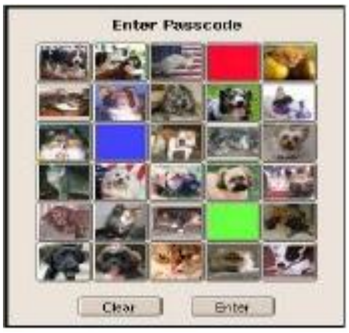


Fig. 1- Cats and dog theme

Fig. 2- Pass faces ^{TM}

Based on the assumption that human can recall human faces easier than other pictures, Real User Corporation has developed their own commercial product named Pass faces TM [5]. Basically, Pass faces (Fig.2a) works as follows, users are required to select the previously seen human face from a grid of nine faces one of which is known while the rest are decoys (Fig. 2). This step is continuously repeated until all the four faces are identified.

passfaces
Sign Up
Welcome to Passfaces
Action
Click on Your Passface
There is only one on the screen.
PREVIOUS
NEXT

Fig .2.a Pass faces : Based on the Brain's Innate ability to Recognize Faces (Fig . By Courtesy)

A comparative study conducted by Brostoff and Sasse [6] in which 34 subjects involved in the test showed that, the Pass faces pass-word is easier to remember compared to textual passwords. Results also showed that Pass faces took a much longer login time than textual passwords. Empirical and comparative studies by Davis et al. [7] showed that, in Pass faces the user's choice is highly affected by race, the gender of the user and the attractiveness of the faces. This will make the Pass faces password somewhat predictable. Sobrado and Birget [8] produced a "moveable frame scheme". This scheme is similar to their previous scheme but, only three pass objects were involved in this technique. One of the pass-objects is placed into the moveable frame. To be authenticated, the user needs to rotate the frame until all the pass-object is locat-ed in a straight line (Fig. 3). To reduce the possibility of logging, Sobrado and Birget suggest repeat of the process a number of times by clicking or turning it randomly. However, this step is un-pleasant, confusing and lengthy since because many non-pass objects are involved. Sobrado and Birget last scheme is called "special geometric configuration". In this scheme four pass objects are involved to form an intersection point (Fig. 4). To be authenticated, user only required to click the object nearest to the intersection point.

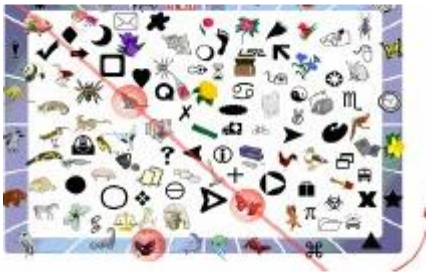


Fig. 3- Moveable frame scheme

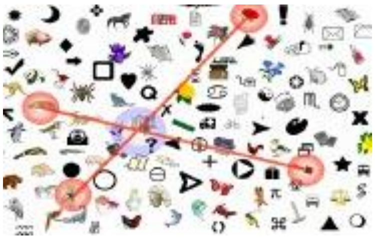


Fig. 4- The special geometric configuration

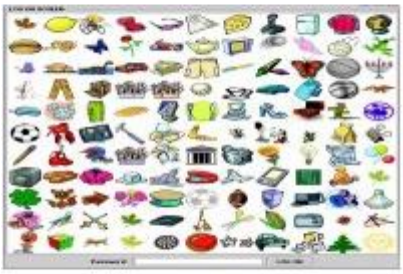


Fig. 5- Pict-O-Lock scheme

Hong et al. [9] proposed a scheme called Pict-O-Lock as shown in Fig. 5. For the purpose of picture memorability, Hong et al. al-lowed users to choose their own words to correlate with each pass -object variant. For example, "3" can be used to be associated with a pass-object alternative which exhibits a shape similar to the shape of "3"; this facilitates the task of password recall. This considerably extends the process of password registration.

Dhamija and Perrig [2] proposed a scheme using a hash visualization technique on the abstract images. The scheme is called "Déjàvu" (Fig. 6). According to their studies, the result showed that it took more time to create a graphical password compared to traditional approach. Besides that, 90% of the authentication using Déjà vu succeeded compared to 70% using the traditional approach. However, due to the larger amount of pictures stored on the server side, the authentication process can be slow due to network traffic delay. Even though the size of the password space of Déjà vu is much smaller compared to text based password, it cannot be concluded that Déjà vu scheme is easy to remember.

Fig. 6- Déjà vu scheme

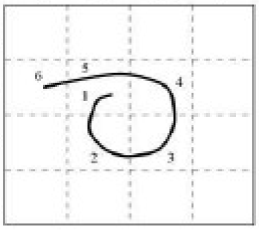


Fig .7 Example of DAS

Recall-Based System

In recall-based systems, the user is asked to reproduce something that he/she created or selected earlier during the registration phase. Recall based schemes can be broadly classified into two groups, viz. pure recall-based technique and cued recall-based technique.

Pure Recall-Based Techniques

In this group, users need to reproduce the passwords without any help or reminder by the system. Draw-A-Secret technique [8], Grid selection [3], and Pass doodle [5] are some examples of pure re-call-based techniques.DAS (Draw-A-Secret) scheme is the one in which the password is a shape drawn on a two-dimensional grid of size G * G as in Fig.7. Each cell in this grid is represented by distinct rectangular coordinates (x, y). The values of touch grids are stored in temporal order of the drawing. If exact coordinates are crossed with the same registered sequence, then the user is authenticated. As with other pure recall-based techniques, DAS has many drawbacks. In 2002, a survey concluded that most users forget their stroke order and they can remember text passwords easier than DAS. Also, the password chosen by users are vulnerable to graphical dictionary attacks and replay attack.

In 2004, the Grid selection technique was proposed by Thorpe and Van Oorschot [3] to enhance the password space of DAS. To improve the DAS security level, they suggested the "Grid Selection" technique, where the selection grid is large at the beginning,

A fine grained grid from which the person selects a drawing grid, a rectangular area to zoom in on, in which they may enter their password as shown in Fig. 8. This technique would increase the

password space of DAS, which improves the security level at the same time. Actually, this technique only improves the password space of DAS but still carries over DAS weaknesses.

Pass doodle, is a graphical password of handwritten drawing or text, normally sketched with a stylus over a touch sensitive screen as shown in Fig. 9. Goldberg et. al have shown that users were able to recognize a complete doodle password as accurately as text-based passwords. Unfortunately, the Pass doodle scheme has many drawbacks. Users were fascinated by other users' drawn doodles, and usually entered other users' password merely to a different doodles from their own. It is concluded that the Pass doodle scheme is vulnerable to several attacks such as guessing, spyware, key-logger, and shoulder surfing.

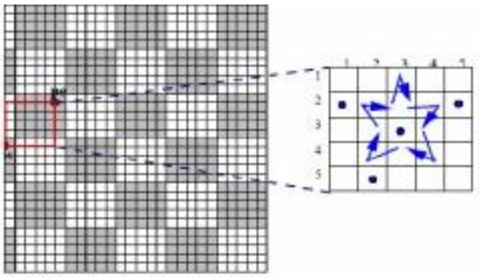


Fig.8 Example of Grid selection

Fig.9 .Example of Pass doodle

Cued Recall-Based Techniques

In this technique, the system gives some hints which help users to reproduce their passwords with high accuracy. These hints will be presented as hot spots (regions) within an image. The user has to choose some of these regions to register as their password and they have to choose the same region following the same order to log into the system. The user must remember the “chosen click spots” and keep them secret. There are many implementations, such as Blonder scheme [1] and Pass-Point scheme [6].In 1996, Recall-based Techniques G. E. Blonder [3] designed a scheme in which a user is presented with a predetermined image. A user has to locate one or more tap regions on the displayed image as their password. The user has to click on the approximate areas of those tap regions in the predefined order (Fig. 10).

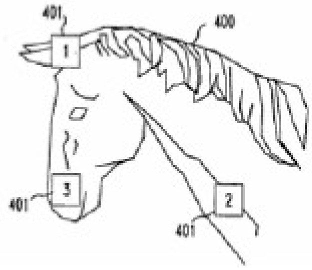


Fig. 10- Blonder scheme

Fig. 11- VisKey SFR

The major problem with this scheme is related to the memorable password space. Users cannot randomly click the background of the image since it will make the created password difficult to recall because of the simple background of the image. VisKey is a recall-based authentication scheme that currently has been commercialized by SFR Company [10] in Germany. This software was designed specifically for mobile devices such as PDAs. In PDA‘s techniques use grid for session password generation [15].To form a password, users need to tap their spots in sequence (Fig. 11).

The problem with this technique is the input tolerance. Since it is difficult to point to the exact spots on the picture, Viskey permits all input within a certain tolerance area around it. The size of this area can be pre-defined by users. Nonetheless, some precautions related to the input precision needs to be set carefully, as it will directly influence the security and the usability of the password. For a practical setting of parameters, a four spot VisKey can offer theoretically almost 1 billion possibilities to define a password. However, is not large enough to avoid the off-line attacks by a high-speed computer. At least seven defined spots are needed in order to overcome the brute force attacks. Passlogix Inc. [11] is a commercial security company located in New York City, USA. Their scheme called Passlogix v-Go uses a technique known as “Repeating a sequence of actions” which means creating a password by a sequence. In this scheme, user can select their background images based on the environment, for example in the kitchen, bathroom, bedroom or etc. (Fig.12) To enter a password, user can click and/or drag on a series of items within that image. For example in the kitchen environment, user can prepare a meal by selecting cooking ingredients, take fast food from fridge and put it in the microwave oven, select some fruits and wash it in washbasin and then put it in the clean bowl.

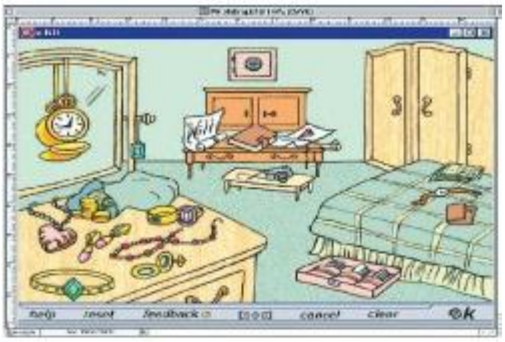
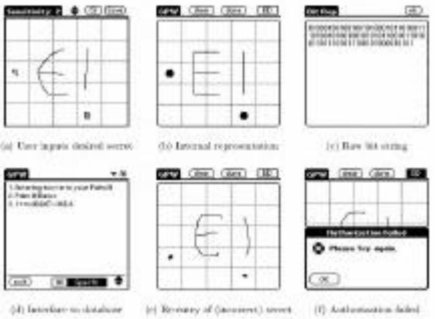


Fig. 12- Passlogix scheme

Fig. 13- Pass points scheme

Other environments such as cocktail lounge allow users to select their favorite vodka, brandy or whiskey and mix it with other cock-tails. This type of authentication is easy to remember and fun to use. Nevertheless, there are some disadvantages such as the size of password space is small. There are limited places that one can take vegetables, fruits or food from and put into, therefore causing the passwords to be somewhat guessable or predictable. Experimental studies by Wiedenbeck et al [12] extended Blonder's design. Their scheme called “Pass Points” expanded the clickable area of the traditional image background introduced by Blonder. As a result, users can click anywhere on an image to form a pass-word (Fig. 13). The tolerance area of each selected location is also calculated to ensure it fulfills the usability and security re-quirements. A user is authenticated if he or she accurately clicks all the selected locations within the tolerance of each selected area. Since the authors allow the usage of any types of images, the amount of memorable password space is relatively larger than textual passwords. Pass Points users had more difficulties to learn the password and it also took more time to input their passwords compared to alphanumeric passwords [12].



(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authentication failed

Fig. 11- Jermyn et al. DAS scheme

Jermyn et al. [13] proposed a scheme, known as “Draw-A-Secret (DAS)”. This scheme is based on a two dimensional grid, users have to draw something to represent their password. Each of the grids coordinates from the drawn pictures is stored in the order of the drawing. To be authenticated, user needs to redraw the picture again. If the drawing lines up at the same grids coordinates with the proper sequence, then the user is authenticated (Figure11). There are some advantages when using a grid as the back-ground for the drawing.

First, the users can draw a password as long as they wish. Second, grid based techniques also lessens the need for the graphical database storage on the server side and reduced the traffic loads without transferring an images through network. Further-more, the full password space for a grid based schemes is much better than traditional textual passwords.

Possible Attack on Graphical Password Techniques Very less study has been done on cracking graphical passwords. Some of the possible techniques for breaking graphical pass-words are given below and a comparison with text-based pass-words.

Brute Force Attack-The main defense against brute force attack is to have a sufficiently large password space. Text-based pass-words have a password space of 94 N, where N is the length of the password, 94 is the number of printable characters excluding SPACE. In some graphical password techniques password space is similar to or larger than that of text-based passwords. Recognition based graphical passwords tend to have smaller password spaces than the recall based methods. A brute force attack is difficult to carry against graphical passwords than text-based passwords. Automatically generated accurate mouse movement is required in brute force attack to reproduce human input, which is mostly difficult in case of recall based graphical passwords.

Dictionary Attacks- Since recognition based graphical pass-words involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords, it is possible to use a dictionary attack but an automated diction-ary attack will be much more difficult than a text based dictionary attack. Overall, graphical passwords are less vulnerable to diction-ary attacks than text-based passwords.

Guessing- Like a serious problem usually associated with text-based passwords, graphical passwords also tend to predict. For example, studies on the Pass face technique have shown that people often choose weak and predictable graphical passwords. Similar predictability is found among the graphical passwords created with the DAS technique. As per Wickelgren

$$\boxed{\mathbf{m - \gamma\ (1+ \beta t\ )^{-\text{€}}}}$$

Where m is memory strength, and t is time (i.e., the retention interval). The equation has three parameters: 1 is the state of long- term memory at t -0 (i.e., the degree of learning), c is the rate of forgetting, and b is a scaling parameter here.

Spyware Attack- Excluding a few exceptions, key logging or key listening spyware cannot be used to break graphical passwords. It is not clear whether “mouse tracking” spyware will be an effective tool against graphical passwords or not. However, mouse motion alone is not enough to break graphical passwords. Such information has to be associated with application information, such as position and size of window, as well as time information. Shoulder surfing: Most of the graphical passwords are vulnerable to shoulder surfing like text based passwords. A few recognition-based techniques are designed to resist shoulder-surfing. Not any of the recall-based based techniques are resistant to should-surfing attack.

Social Engineering- To give away graphical passwords to another person is difficult as compared to text based password. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

II. Conclusion and Future Directions

A study of existing graphical password techniques is done in this paper. The graphical password techniques are classified into two categories; recognition-based and recall-based techniques. Over-all, it is more difficult to break graphical passwords using the established attack methods like brute force attack, dictionary attack ,and spyware. The past decade has seen an emergent interest in using graphical passwords as an alternative to the conventional text-based passwords. There is a need for more in-depth research that investigates possible attack methods against graphical pass-words.

Acknowledgement

We express sincere gratitude to our guide for providing their valuable guidance and necessary facilities needed for the successful completion of this paper throughout. We thank our parents for their support and thank all our friends and well-wishers who were a constant source of inspiration

References

[1] Adams A. and Sasse M.A. (1999) Communications of the ACM, 42, 41-46.
[2] Dhamija R. and Perrig A. (2000) In Proceedings of the 9th USENIX Security Symposium.
[3] Blonder G. (1996) In Lucent Technologies, Inc., Murray Hill, NJ, United States Patent 5559961.
[4] Jansen W., Gavrila S., Korolev V., Ayers R. and Swanstrom R. (2003) NISTt NISTIR 7030.
[5] Real User Corporation (2007) Passfaces T M , http//:www.realuser.com.
[6] Brostoff S. and Sasse M.A. In People and Computers XIV – Usability or Else: Proceedings of HCI. Sunderland, U.K, 2000.
[7] Davis D., Monrose F. and Reiter M.K. (2004) Proceedings of the 13th USENIX Security Symposium. California.
[8] So brad o L. and Bi rg et J. (200 7) ht tp: // rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbi rg.htm.
[9] Hong D., Man S., Hawes B. and Mathews M. (2004) Interna- tional conference on security and management, Las Vergas, NV.
[10] SFR IT-Engineering (2007) http://www.sfrsoftware. de/cms/ EN/pocketpc/viskey/.
[11] Passlogix (2007) http://www.passlogix.com.
[12] Wiedenbeck S., Waters J., Birget J.C., Brodskiy A. and Memon N. (2005) International Journal of Human-Computer Studies, 63, 102-127.
[13] Jermyn I., Mayer A. Monrose F., Reiter M.K. and Rubin A.D. (1999) In Proceedings of the 8th USENIX Security Symposi- um.
[14] Sarita Yardi , Nick Feamster , Amy Bruckman School of Computer Science,School of Interactive Computing Georgia Institute of Technology , yardi,feamster,asb@cc.gatech.edu WOSN'08,August 18, 2008, Seattle, Washington, USA
[15] M.sashi ,M.Sreelatha ,M.Anirudh,Md.Sultan Ahamer, V.Manoj kumar ,IJNSA , Dept.of CSSE,Andhra university, india
[16] Wixted, J.T., & Ebbesen, E. (1991). On the form of forgetting. Psy-chological Science , 2 , 409–415