Secure Authentication by Graphical Password

Shinde Swapnil K, 1, Patil Yogesh N. 2
Department of Computer Engineering
1Student M.Tech. at Dr. Babasaheb Ambedkar Technological University, Lonere, (M.S.) India
swapnilkshinde7@gmail.com

Abstract- The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords because according to human psychology human can easily remember pictures. In this paper we had done the study of various graphical password authentication techniques and turned our way of think to use advantages of selected authentication techniques to build the system which provide stronger security and having high usability.

Keywords – Multifactor Authentication, Textual Password, Graphical password, Security attacks.

I. INTRODUCTION

The current situation where many passwords used in practice are either weak- and-memorable or secure-but difficult-to-remember, despite the need for secure and memorable passwords. The term Authentication describes the process of verifying the identity of a person or entity. It is the process of determining whether someone or something is, in fact, who or what it is declared to be. Authentication methodologies are numerous and range from simple to complex. The level of security provided varies based upon both the technique used and the manner in which it is deployed. The most prevalent form is probably the authentication with a user name and a password. Unfortunately it is also one of the most insecure methods. There is an unlimited range of variations of how a user can be authenticated to a web application. Some of the most popular ones are going to be described in the following.

Authentication methods can involve up to three factors:

1. Knowledge: What a user knows (i.e., a password or challenge question)
2. Possession: What a user has (i.e., a security token or mobile phone)
3. Attribute: What the user is (i.e. biometric characteristics like a fingerprint or the pattern of the eye)

Possession based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

Strong authentication is also commonly referred to as two-factor authentication or multi-factor authentication. This alludes to the fact that there is more than one factor, or proof, needed in order for an authentication to be made. When only one factor is utilized to authenticate a user, it is considered to be a weak form of authentication. Multi-factor authentication may include multiple types of the same authentication method (for example, two static passwords) but would not necessarily be considered strong authentication.

The rest of the paper is organized as follows. Literature survey in Section II. Our proposed scheme III. Concluding remarks are given in section IV.

II. LITERATURE SURVEY

Graphical passwords are an alternative type of knowledge-based authentication. In graphical passwords, images or visual representations are used instead of alphanumeric characters. The premise behind graphical passwords is that humans have better memory for images than text.

The graphical passwords are divided in two parts.
A. Recognition based

B. Recall based

A. Recognition Based

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.

a. In dej a Vu [1], users select and memorize a subset of images from a larger sample to create their portfolio. To log in, users must recognize images belonging to their pre-defined portfolio from a set of decoy images; in the test system, a panel of 25 images is displayed, 5 of which belong to the user's portfolio. Users must identify all of images from their portfolio and only one panel is displayed. Images of 'random art' are used to make it more difficult for users to write down their password or share it with others by describing the images from their portfolio.

b. In Pass Faces [2], users pre-select a set of images of human faces. During login, they are presented with a panel of candidate faces and have to select the face belonging to their set from among decoys. This process is repeated several times with different panels, and users must perform each round correctly in order to successfully authenticate themselves. In the test systems, a panel consisted of 9 images, one of which belonged to the user's portfolio, and a user completed 4 rounds to login.

c. Story was proposed by Davis et al. [3] A comparison system for Pass Faces. In Story, users first select a sequence of images for their portfolio. To log in, users are presented with one panel of images and must identify their portfolio images from among decoys. The images contained everyday objects, places, or people.

Story also introduced a sequential component by requiring that users select their images in the correct order. To help with memorability, users were instructed to mentally construct a story to connect the images in their set. In the test system, a panel contained 9 images and a user's password consisted of a sequence of 4 images selected from within this panel.

As per the study of all above recognition based techniques suffer from shoulder surfing problem, some researchers had suggested new techniques resistant to shoulder surfing attack.

d. Sobrado and Birget [4] developed a graphical password technique that deals with the shoulder surfing problem. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. In order to make the password hard to guess, Sobrado and Birget[4] suggested using 1000 objects, which makes the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large.

e. Man, et al.[5] proposed another shoulder-surfing resistant algorithm. In this algorithm, a user selects a number of pictures as pass-objects. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass objects in reference to a pair of eyes.

![Fig 1. Man et Al. approach.](image-url)
Secure Authentication by Graphical Password

B. Recall Based

- Pure Recall based Authentication –

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.

  a. Jermyn, et al.[6] proposed a technique, called “Draw - a - secret (DAS)”, which allows the user to draw their unique password. A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated.

  b. Thorpe and van Oorschot [7] analyzed the memorable password space of the graphical password scheme by Jermyn et al. They introduced the concept of graphical dictionaries and studied the possibility of a brute-force attack using such dictionaries. They defined a length parameter for the DAS type graphical passwords and showed that DAS passwords of length 8 or larger on a 5 x 5 grid may be less susceptible to dictionary attack than textual passwords. They also showed that the space of mirror symmetric graphical passwords is significantly smaller than the full DAS password space. Since people recall symmetric images better than asymmetric images, it is expected that a significant fraction of users will choose mirror symmetric passwords.

  c. Goldberg et al.[8] did a user study in which they used a technique called “Passdoodle”. This is a graphical password comprised of handwritten designs or text, usually drawn with a stylus onto a touch sensitive screen. Their study concluded that users were able to remember complete doodle images as accurately as alphanumeric passwords. The user studies also showed that people are less likely to recall the order in which they drew a DAS password.

- 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.

  a. Blonder [9] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as with a text-based password).

  b. The “PassPoint” system by Wiedenbeck, et al.[10-12] extended Blonder’s idea by eliminating the predefined boundaries and allowing arbitrary images to be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence.

These various authentications suffer from various security attacks. We divided them with respect to security attacks. As shown in table 1.

Solutions- The various graphical authentication systems are resistant to shoulder surfing if they use a keyboard as input medium to enter the password rather than the mouse. If they uses mouse then the behavior of the mouse can be captured by screen scrapper malicious software and your password get disclosed after 2-3 login times. While select the complex pictures or the random art images so the password cannot be get easily shared and become resistant to Social engineering attack.

III. PROPOSED SCHEME

Study of all above existing password systems has their own advantages and drawbacks. So we concluded to make use of multifactor password authentication system by considering multiple factors introduced in section I. in our proposed scheme we are using three knowledge base factors (i.e. one textual and two graphical passwords) and one personal (biometric) authentication factor to make authentication system more and more secure. to get authenticate
from our system user need to pass from three types of hurdles and we concentrated different security factor at different level.

**Factor 1-** In which we considered a textual password. It must be satisfy all the standard criteria of the textual password. It must be a combination of alphabets, numbers, and special symbols and length must not be less than 8 characters.

**Advancement** – we are doing 128 bit encryption before storing that password in server side database. Due to this if somebody make attack on server to pirates the password but the pirated passwords becomes useless due to encryption.

**Factor 2-** In this factor we are using a Recognition base Graphical password which is resistant to shoulder surfing attack and resistant spyware, screen scrapper as well as social engineering, difficult to guess and Dictionary attack.

We are extending here the authentication technique suggested by man et al. [5]. We are making some advancement in that to make it resistant to Man-In-Middle attack.

Man et al. given a unique number to every object on the screen and at the time of registration user select the images from the screen and remember the unique number associated with that image at the of authentication user need to enter that unique number associated with registered object. This system is resistant to shoulder surfing but vulnerable to man in middle attack. So we had made some changes.

**Advancement-** Rather than giving a unique number to every image on the screen and create old problem of remembrance. We are assigning a random number to image and numbers on that images are changes randomly from login to login and also changes the positions of the images on the screen. At the time of registration user enters the numbers shown on image as password but need to be concentrate only on images not on the number. Because we are creating purely image dependent system. The numbers entered by user get stored at back end in server. When user comes for login he sees a different numbers associated on images. He need to search out his registered images need not to worry about numbers. Enter numbers associated with those images.

**Factor 3-** In third factors we are using cued click recall based technique with the integration of sound signature. As this technique Is already suggested by Saurabh Singh [13] this technique suggest that user need click on more than one images rather than giving multiple click on single image so this technique is very difficult to guess and sound signature allows user to easily remember the password.

**Why this?** This technique is having more than one click but not on the single image. It having more than one click on number of images, so it have large password space, can’t be easily guessed and includes with that a sound signature. Means after every click on image it generates sound. If click is correct then generates particular sound if not then generate random sound. Means this technique is strongly resistant to well known phishing attack.

The flow of scheme at the time of authentication –

1. User enters a username and textual password. If user entered correct text password then allows to user to enter in second step and shows the correct image portfolio as he selected during registration. Otherwise system allows the user to enter in second step but shows different image portfolio than selected during registration. And onto onwards that system allows completing all steps but not performing authentication at any step and at last shows message authentication failed.

2. In second step user needs to enter recognition based graphical password by entering a random number on the image as he selected the image at registration but must be in the sequence. If user entered password correct then allows to enter third step and authentication in third step get activated and shows correct images for third step as he selected during registration. If user entered wrong password then allows entering in third step but authentication is deactivated. And user finally get message authentication failed.

3. In third step we are using cued click recall base authentication with the integration of sound signature. It generates sound after every click by the user. If it click correctly then generate the correct sound otherwise generate random sound.
Secure Authentication by Graphical Password

<table>
<thead>
<tr>
<th>Security Attack</th>
<th>Authentication Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shoulder Surfing Attack</td>
<td>Dej vu, Pass faces, Pass point, Story, pass Doodle, Blonder Scheme, and current Android Locking system.</td>
</tr>
<tr>
<td>Man in middle</td>
<td>Textual password, pass faces, story, man et al., soberbo and birgret scheme,</td>
</tr>
<tr>
<td>Spyware</td>
<td>Dej vu, Pass faces, Pass point, Story, pass Doodle, Blonder Scheme, and current Android Locking system.</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Pass faces, Pass point, Story, pass Doodle, Blonder Scheme, and current Android Locking system.</td>
</tr>
</tbody>
</table>

IV. CONCLUSION

We had done the study of various password authentication techniques and carried out our own approach to make the combination of various best authentication system with their advantages at the different levels of authentication.

Our proposed approach is resistant to shoulder surfing, man in middle and strongly resistant to phishing and dictionary attack, social engineering. We are developing our proposed scheme for web service applications and also trying to apply it for folder locking. Currently we are working for third step and considered biometric or personal authentication as last factor.

REFERENCE

[8]. J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better Authentication,” presented at
[13]. International Journal of Computer Applications (0975 – 8887)