The Recognition and Recall Approach based Graphical Password Technique

Aakansha Gokhale
Dept.of Information Technology
Dr. D. Y. Patil Polytechnic, Nerul
Navi Mumbai, Maharashtra
India

Vijaya Waghmare
Dept.of Computer Engineering
Saraswati College Of Engineering, Kharghar
Navi Mumbai, Maharashtra
India

ABSTRACT

Today Information Technology has become a part of our everyday life. Information Technology means use of computers and internet to store, retrieve, transmit and manipulate the information. So all the organizations, industries and also every individual are using computers to store and share/communicate the information. So here security is very much important while storing and communicating the information. Security means protecting computers, networks, programs and information from unintended or unauthorized access, change or destruction. For this security various techniques are available. Among them the most common and easy to use is a password. It can be considered as a principal part of authentication process. The traditional password technique is a textual password. But there are various deficiencies in this password. It is vulnerable to various attacks. So to overcome these limitations alternative technique is introduced which is graphical password. As name indicates, in this, various images/pictures are used as a password. But it is observed that because of graphic nature nearly all the graphical passwords are vulnerable to shoulder surfing attack. To overcome this here a new graphical password authentication technique is developed which is a combination of recognition and recall approach based techniques. It is also resistant to other types of attacks to some extent.It can be useful for smart phones, PDA, iPod, iPhone etc.

General Terms

Computer Security, Password

Keywords

Authentication, Graphical Password, Shoulder Surfing, Textual password.

1. INTRODUCTION

1.1 Overview

The traditional method of security is to use textual password. It is also called as alphanumeric password as it is a combination of alphabets, digits and special symbols. But it is vulnerable to various attacks like brute force, dictionary attack, easy to guess, social engineering, spyware, keylogger, hidden camera, shoulder surfing etc.

So to overcome these limitations of textual password an alternative technique is developed which is a graphical password [1].

1.2 Graphical Password

In this, images or pictures are used as a password instead of text. Also it is psychologically proven that images can be easily memorized by human [2-5]. It is resistant to social engineering, dictionary attack, keylogger because images are used as a password.

It has two categories: Recognition based and Recall based. In recognition based images are recognized by user during authentication and in recall based images are recalled by user during authentication.

Thus, as images are used as a password here, it is easy to remember for user and difficult to guess for attacker.

But because of graphic nature it has also some drawbacks. And the major drawback observed is nearly all the graphical password techniques are vulnerable to shoulder surfing attack. It means in this attack any malicious user can observe the password across the shoulder of user while he enters it.

Theproposed and implemented technique here is resistant to shoulder surfing attack to some extent. It is a combination of recognition and recall approach based techniques.

The paper is organized as follows. The section II explains various existing graphical password techniques. The section III consists of the detailed explanation of new implemented technique. The analysis of new technique is done in section IV. The section V concludes the paper with some further discussions.

2. BACKGROUND AND RELATED WORK

Lots of graphical password techniques have been developed in earlier days. Actually graphical password was introduced by Blonder in 1996. This section is the brief overview of recognition and recall approach based techniques.

2.1 Recognition based techniques

In these techniques some images are shown to the user during registration. The user has to select some images from the number of images. Afterwards as name indicates for valid login user has to recognize those preselected images in a correct sequence.

Some examples of this are:

2.1.1 Dhamija and Perrig technique [6]

Here, during registration user selects some number of images from a set of random images. For authentication user has to recognize those selected images in a sequence.

2.1.2 Passface Technique [7]

In this, during registration human face database is shown to the user. The user has to select the four faces according to his choice from the database. During login, a grid of nine human faces is shown to the user. In this grid one is the known face and others are the decoy faces. User has to recognize that known face. This is repeated for four times to recognize four human faces registered earlier.

2.2 Recall based techniques

In these techniques, user has to recall something that has been created or selected during registration.

2.2.1 Pure recall based techniques

Here user is not provided a clue to recall a password.

Some examples of this are:

2.2.1.1 Passdoodle technique [8]

Here some handwritten text/design is drawn by the user on touch sensitive screen with stylus. During login user has to redraw the same text/design.

2.2.1.2 Signature technique [9]

Here, during registration user has to register his own signature. For authentication user has to draw the same signature with mouse.

2.2.2 Cued recall based techniques

As name indicates, in these techniques, a clue (hint) is provided to the user to recall a password. Hence these techniques are easier than pure recall based techniques.

Some examples of this are:

2.2.2.1 Blonder technique [10]

In this, for password registration a predetermined image with predetermined tap regions are displayed to the user. The user has to click inside those tap regions in a sequential manner. For authentication, user has to click approximate areas of those tap regions in a predefined sequence. Here image is a clue to recall a password.

2.2.2.2 Passpoints technique [11]

In this technique, any natural picture or painting is used for click points. For creation of password user can click anywhere on a picture. The tolerance around each click point is calculated. For authentication, user has to click within the tolerances of click points in a sequence.

All the above techniques have been studied on the basis of security and usability metrics. It is observed that some techniques are strongly secure but not easy to use. On contrary, some techniques are user friendly but not provide strong security. Also a common observation about all the techniques is that they are not strongly resistant to shoulder surfing attack.

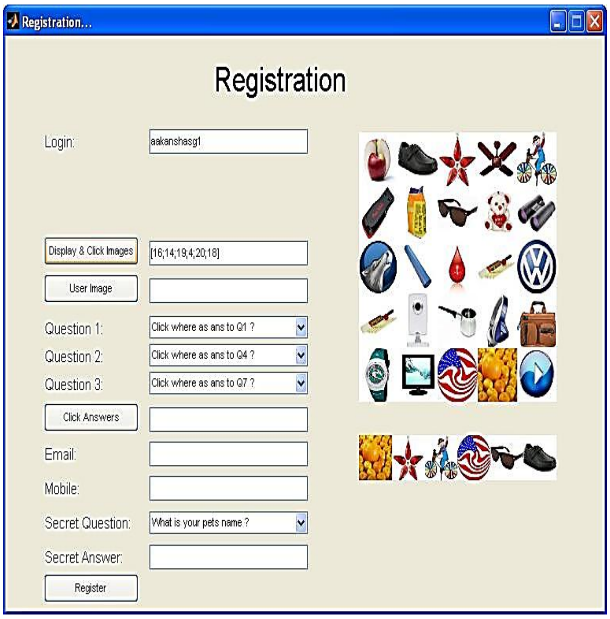
The proposed and implemented technique here is easy to use as well as resistant to shoulder surfing and also to other types of possible attacks to some extent.

3. PROPOSED AND IMPLEMENTED SYSTEM

This technique is a combination of recognition and recall approach based techniques. It has two phases. First is a registration phase and second is a login phase.

3.1 Registration Phase

1. The user enters the username.
2. A grid of 25 images is displayed to the user. User will select some images from this grid to set as a password which is called as a secret pass. The minimum number of selected images should be six. Also it should contain the even number of images to form the pairs of images. These secret pass images are displayed in one panel below the grid of images so that user can be easily remembered and confirmed the selected images in a sequence. For security it will disappear after five seconds. It is shown in Figure1. A session password is generated from this secret pass. This session password is a step-I authentication password.



Login: aakanshasgl

[16;14;19;4;20;18]

Question 1: Click where as ans to Q1 ?

Question 2: Click where as ans to Q4 ?

Question 3: Click where as ans to Q7 ?

Email:

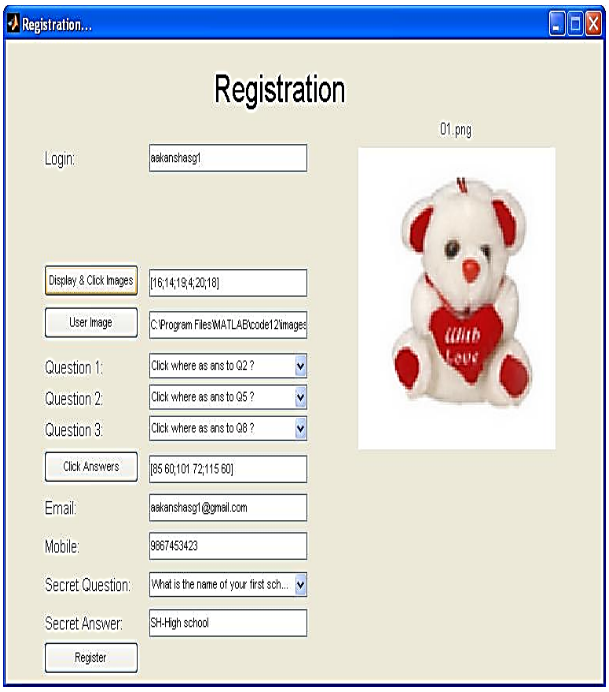
Mobile:

Secret Question: What is your pets name ?

Secret Answer:

Figure 1: Registration for step-I

3. After this user will select one image from an image database or from a local memory.
4. Then question set and this image is displayed to the user. The user has to select any three questions randomly from this set.
5. As an answer of these three questions user has to click on three different points on the image. The single click point is called as a ROA (Region of Answer). So there are three different ROAs. These ROAs is the step-II authentication password. It is shown in Figure2.
6. Afterwards user has to register email-id, mobile number. Also user has to select one secret question from a set of questions and its related secret answer. It is also shown in Figure2. This is useful if user forgets any password that password will be mailed to user's registered mail-id. To check the validity of the user secret question and its secret answer will be used.



Registration...

Registration

01.png

Login: aakanshasg1

[16;14;19;4;20;18]

C:\Program Files\MATLAB\code12\images

Question 1: Click where as ans to Q2 ?

Question 2: Click where as ans to Q5 ?

Question 3: Click where as ans to Q8 ?

[85 60;101 72;115 60]

Email: aakanshasg1@gmail.com

Mobile: 9867453423

Secret Question: What is the name of your first sch...

Secret Answer: SH-High school

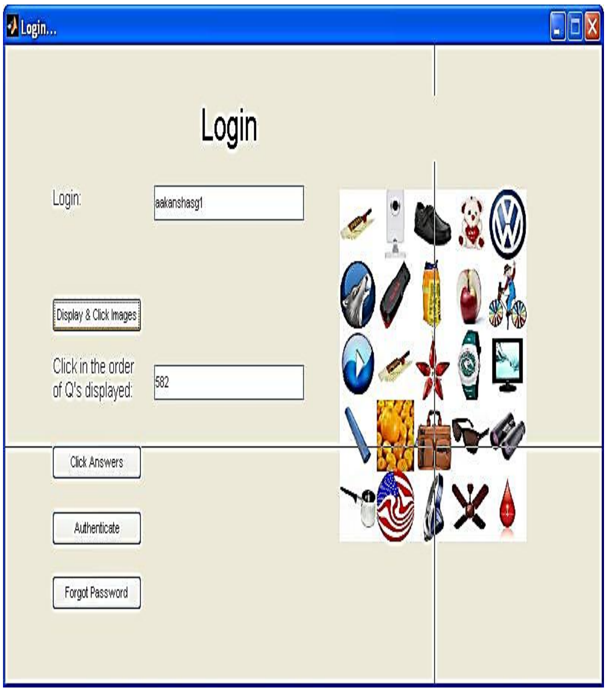
Figure 2: Registration for step-II

3.2 Login Phase

1. The step-I authentication is based on recognition based approach. First, user has to enter the correct username. After this for step-I graphical password the grid of 25 images is shown to the user. For every login the image positions in a grid will change. As explained earlier a session password is based on the secret pass. For generating a session password, user has to form the pairs of images in secret pass .In pair, first image is used to select the row and the second image is used to select the column. The intersection image is a part of session password. It is repeated for all pairs in secret pass. E.g. in secret pass in first pair suppose, the first image is oranges and second image is star, so the first intersection image in secret pass is bag. This is shown in Figure3. As image positions will vary at every login, the session password will also vary at every login. So it is very difficult for any unauthorized user to guess the step-I password.

2. Only after successful authentication of step-I, user can go for step-II authentication. It is based on cued recall based approach. For this, the preselected image and preselected three questionsare used as clues. Also whole questions are not displayed here. Instead, only three question numbers are shown as a single three digit number. E.g. 582 as shown in Figure4.Also the order of question numbers will vary at every login. This adds strong security for step-II password. The user has to click the correct ROAs (center and some tolerance in both X and Y axis) according to order of question numbers. Because of randomization of question numbers guessing of step-II password is also very difficult for any imposter.

3. After successful selections in step-II password user is an authorized user to access the system



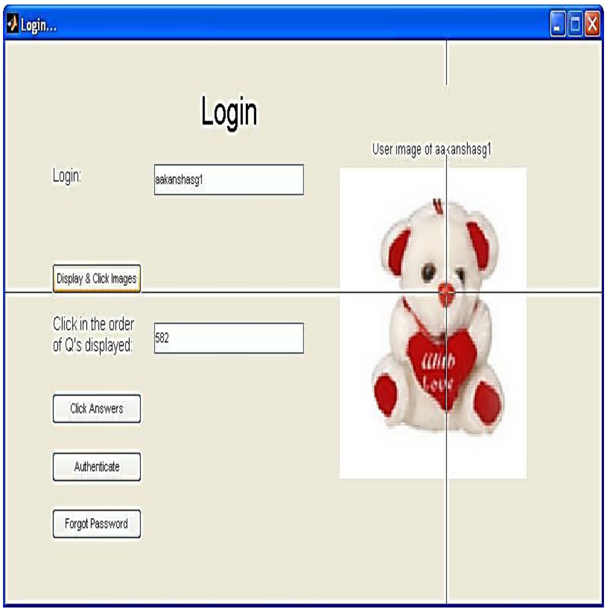
Login...

Login

Login: aakanshasg1

Click in the order of Q's displayed: 582

Figure 3: Authentication for step-I



Login...

Login

Login: aakanshasg1

User image of aakanshasg1

Click in the order of Q's displayed: 582

Figure 4: Authentication for step-II

Thus step-I and step-II passwords are very difficult to guess for anyone but easy to remember and access for user. This makes the system strongly secure as well as easy to use. Thus thesystem satisfies both security and usability metrics.

4. ANALYSIS

As this system is a combination of two types of graphical passwords and also it has a large password space, it is strongly resistant to brute force and guessing attacks.

For step-I login the password space is:

$$3 * (25\ C\ 2) = \frac{(3 * 25!)}{(2! * 23!)} = 900\ Passwords$$

Above figure is without random shuffling. With random shuffling the password space is:

P_1= 900 * 25! = 1.39*10^{28}> 10^{28} Passwords.

For step-II login the password space is:

The X×Y is the size of image and q is the maximum number of questions selected, For each question the size of click area is z × z.

So the password space is:

$$P_2 = \sum_{i=1}^{q} (i! \times [\frac{X \times Y}{z^2}]^i)$$

E.g. Consider the size of the image is 200 × 200; the maximum numbers of questions selected are 3 and suppose the size of the click area (ROA) is 20 × 20,

So P_2=6020100.

So available password space by combining two steps is:

$P=P_1 \times P_2$

P=(1.39 * 10^{28}) × 6020100 =8.367939e+34

Thus the system provides strong security against brute force attack as it has large password space.

This system also provides security against shoulder surfing attack.

In step-I login; there is a randomization of 25 images at every login. So session password will change at every login. Also 25 images are displayed as a thumbnail size. So it is very difficult for any attacker to remember the step-I password by seeing it only once.

For step-II authentication, the order of question numbers will vary and it is displayed as a single three digit number.

So because of randomization in both the steps attacker can get confused if he is trying to remember the password.

Also if any user forgets any password it is mailed to user's registered mail id. But here authenticity of the user must be proven by answering the secret question correctly. Then only he will receive the password on his registered mail id.

But this also adds security to our system. If any imposter trying to get the password, it is unable for him to get both the passwords. So he may go for forget password option to get the password details. But here also authenticity has to be proven by answering the secret question correctly.

In this way, the system is strongly secure against various attacks but easy to use.

5. CONCLUSION AND FUTURE DISCUSSIONS

This system is a combination of recognition and recall based approach. It is more usable and secure as compare to previous graphical password authentication systems.

As password space is very large it provides the security against brute force attack. It is easy to use. Passwords can be created and memorized easily.

Randomization in both the authentication steps provides strong security against shoulder surfing.

Overall the system is resistant to all other possible attacks also. This system can be used for highly secure systems.

In future, one more addition possible to the system is, if the user forgets any password that password is mailed to user's registered mail id and such a message will be sent to user's registered mobile number also.

The second addition possible is if any unknown user is trying to get the passwords of system, it may possible that after five unsuccessful attempts, for a next sixth attempt a dummy window of application, for which, this system is used for security; is displayed to that user. So he thinks that he is successful to get the passwords. But at the same time the photo of that person will be captured by the system and will be sent to authorize user's registered mobile number. So he will get alert about the system and he can give the instructions regarding this unauthorized access to admin.

In this way, user can get the system updates although he is offline.

Thus, in future this system can be made more and more secure but easy to access.

6. REFERENCES

[1] XiaoyuanSuo, Ying Zhu, G.Scott. Owen, "Graphical Passwords: A Survey", Department of Computer Science Georgia State University.

[2] Kirkpatrick. "An experimental study of memory".PsychologicalReview, 1:602-609, 1894.

[3] S. Madigan. "Picture memory". In J. Yuille, editor, *I*magery, Memory, and Cognition: Essays in Honor of Allan Paivio, chapter 3, pp.65-89. Lawrence Erlbaum Associates, 1983.

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

[5] R. Shepard. "Recognition memory for words, sentences, and pictures". *Journal of Verbal Learning and Verbal Behavior*, 6:156-163, 1967.

[6] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9 USENIX Security Symposiums, 2000.

[7] Real User Corporation, "How the Passface System Works", 2005.

[8] Christopher Varenhorst" Passdoodles; a Lightweight Authentication Method ", Massachusetts Institute of Technology, Research Science Institute, July 27, 2004.

[9] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written withMouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[10] G. E. Blonder. Graphical passwords. United States Patent5559961, 1996.

[11] Susan Wiedenbeck, Jim Waters, Jean- Camille Birget and Alex Brodskiy, NasirMemon. PassPoints,"Design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, 63(1-2): 102-127, July 2005.