Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 490 – 498

Procedia
Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

The Shoulder Surfing Resistant Graphical Password Authentication Technique

Mrs.Aakansha S. Gokhale[a], Prof. Vijaya S.Waghmare[b]

[a]Lecturer,Department of Information Technology,Dr.D.Y.Patil Polytechnic,Nerul, Navi Mumbai,400706,India
[b]Asst. Professor,Department of Computer Engineering,Saraswati College of Engineering,Kharghar,Navi Mumbai,410210,India

Abstract

Nowadays computer as well as information security is the most significant challenge. Authorized users should access the system or information. Authorization can't occur without authentication. For this authentication various techniques are available. Among them the most popular and easy is the password technique. Password ensures that computer or information can be accessed by those who have been granted right to view or access them. Traditional password technique is a textual password which is also called alphanumeric password. But these textual passwords are easy to crack through various types of attack. So to overcome these vulnerabilities, a graphical password technique is introduced. As name suggests in this technique images (pictures) are used as a password instead of text. Also psychological study says that human can easily remember images than text. So according to this fact, graphical passwords are easy to remember and difficult to guess. But because of graphic nature, nearly all the graphical password techniques are vulnerable to shoulder surfing attack. So here, a new graphical password authentication technique is proposed which is resistant to shoulder surfing and also other types of possible attacks to some extent. It is a combination of recognition and recall based approach. It can be useful for smart held devices like smart phones, PDA, iPod, iPhone etc.

Keywords: Authorization; Graphical Password; Security; Shoulder surfing

doi:10.1016/j.procs.2016.03.063

1. Introduction

1.1. Overview

Today, authentication is achieved through the use of password technique. To prove and maintain the identity every user uses a password authentication [1]. The traditional method of password is a textual (alphanumeric) password. It is the combination of alphabets, digits and special symbols. But it has various limitations. To remember easily, here the passwords are kept short and simple like personal names, family member names, birth dates, pet names, phone numbers etc. and so vulnerable to various types of attacks like easy to guess, brute force, dictionary attack, shoulder surfing, hidden camera, social engineering and malicious softwares like keylogger, spyware etc.

To overcome these limitations users can use the strong (complex) password. But it is difficult to remember. So to memorize easily users write the password on paper and so it is easily available to anyone.

Also nowadays various accounts are maintained by users for various purposes like personal computer, social network, email, online transactions etc. and to remember easily users can use the same password for all accounts and it reduces the security [2].

So to reduce the shortcomings of textual passwords a new technique is developed which is a Graphical Password [3].

1.2. Graphical Password

As name indicates in this, various types of images or shapes are used as password. Also psychological study says that images can be easily remembered by human than text [4 -7]. Human brains can process images easily. Because of this human characteristic, graphical passwords are superior to textual passwords. As images are used it is resistant to dictionary attack, keylogger, social engineering etc.

There are two types of graphical password techniques: Recognition based and Recall based.

In Recognition based, various images are presented to the user and from that user has to recognize the right images in a correct sequence. In Recall based, user has to reproduce something that he/she has been created or selected during registration.

So, as images are used in graphical password it is easy to remember and difficult to guess and it is best alternative for textual password.

But it is observed that there are also some limitations of graphical password techniques and the major limitation observed is that, it is vulnerable to shoulder surfing attack as images are used as a password. Shoulder surfing means watching over the person’s shoulder to get the password. When user enters password using keyboard, mouse, touch screen or any other traditional input device, a malicious observer may be able to acquire the user’s password credentials.

Our proposed technique is resistant to shoulder surfing to some extent and also to other possible attacks. It is a combination of recognition and recall based approach.

The paper is organized as follows. Section II is the review of some existing graphical password techniques. Section III explains the existing system. Section IV comprises our proposed system. Section V analyses proposed system. Section VI concludes the paper with some future additions.

2. Related work

A lot of research work has been done for graphical password techniques. Originally it was introduced by Blonder in 1996. This section is a brief overview of recognition and recall based techniques.

2.1. Recognition Based Techniques

In this, user is presented with a set of random images during registration. The user has to select the particular number of images from this set as a password. During authentication, user has to recognize those preselected images in a correct sequence.

Some examples of this are:

2.1.1 Jensen et al. technique [8]: This technique is proposed for mobiles, PDAs. First user is required to select a theme (E.g. Cats and Dogs, Sea and Shore etc.). Images based on theme are shown to user in 5 x 6 grid and also each image is displayed in thumbnail size. To form a password user has to select the images in a sequence. The user needs to recognize the previously selected images and touch it using stylus in a correct sequence for authentication.

The number of images here are limited only to 30, so the size of the password space is small. A number is assigned for each image and a sequence of selection will produce a numerical password. Sometimes this numerical password is shorter than the textual password. So to overcome this problem user can select two images at a time on single click to increase a password space size. But this will become more difficult and complex for user.

2.1.2 ImagePass technique [9]: In this, during registration user is presented with a grid of 30 images. The user has to select images as a password.

During login user is presented with a grid of 4 x 3 which is a combination of real and decoy images. From the grid user has to select the real images in a correct sequence for authentication. The image positions will vary at every login.

It is not strongly resistant to shoulder surfing as grid is only of size 4 x 3 and also the password images are fixed. So those can be easily seen and remembered by attacker.

2.1.3 ColorLogin technique [10]: In this, background color is used to decrease the login time. Multiple colors are used to confuse the imposters, but easy to use for authorized users. It is resistant to shoulder surfing attack but the password space, here, is less than text-based password.

2.2. Recall Based Techniques

In this, during login phase user is asked to recall (reproduce) something that he/she has created or selected during the registration phase.

It has two categories:

2.2.1 Pure Recall Based Techniques: In this, user is not provided a clue to recall a password.

Some examples of this are:

2.2.1.1 Passdoodle technique [11]: It is a handwritten design or text, usually drawn with stylus onto touch sensitive screen.

The users can be easily remembered the passdoodle drawn by them like textual password, but it is observed that sometimes the users forget the order in which they draw a doodle. Also sometimes users were fascinated by the doodles drawn by the other users and entered other users login details. This is vulnerable to guessing, spyware, shoulder surfing attacks.

2.2.1.2 Draw-a-Secret (DAS) technique [12]: In this technique, user can draw a picture on a 2D grid of size G x G. Each cell is denoted by discrete rectangular coordinates (x, y). The values of touch grids are stored in the order of drawing. For authentication, user has to redraw the same picture touching the same coordinates of a grid. In this, users can draw a password as long as they wish. The password space is much better than textual password.

Limitation here is users can forget their stroke order and so sometimes it is easier to remember the text password than DAS password. Also users sometimes choose a frail password, which is vulnerable to graphical dictionary attack and replay attack.

2.2.1.3 Signature technique [13]: The user is authenticated by drawing signature using mouse. There is no need to memorize the signature and also signatures are hard to fake.

But everybody is not familiar with using mouse as a writing device. It is difficult to draw the signature in the same perimeter as at the time of registration. One solution to this is to use pen like input device. But such devices are not widely use and adding new device to current system can be expensive.

2.2.2 Cued Recall Based Techniques: In these techniques, for authentication, a clue is provided to user to recall a password, registered during registration phase. These techniques provide hints to user to memorize the password hence easier than pure recall based techniques.

Some examples of this are:

2.2.2.1 Blonder technique [14]: The graphical passwords were originally described by Blonder. In this, a predetermined image with predetermined tap regions is shown to the user. During registration, for password creation user has to click those tap regions in a particular sequence. For authentication, user has to click the approximate areas of those tap regions in the predefined sequence. The image can assist the user to recall the password and so this scheme is considered as more convenient than textual password.

The drawback of this is memorable password space. The user cannot click where he wants because of predetermined tap regions. Also background of image is very simple.

2.2.2.2 PassPoints technique [15]: To overcome the limitations of Blonder technique, this technique was proposed. In this, any natural picture/painting is used, which helps the user to remember the click points. Here no need of predefined click points like Blonder technique. During registration, to create a password user can click on any place on the image. The tolerance around each chosen click point is calculated. For authentication, user has to click within tolerances of chosen click points in a correct sequence.

Here, password is easily created but the users can have more difficulty in learning their passwords than textual passwords. Also login time is larger than textual password.

2.2.2.3 Passlogix V-Go technique [16]: Passlogix Inc. is a commercial security company located in “New York City, USA”. This scheme is also known as “Repeating a sequence of actions” which means creating a password by navigating through an image such as in the kitchen, bathroom, bedroom or others. E.g. 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 put it in the clean bowl.

But limitation here is the size of password space is very 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.

All the above mentioned techniques have been studied on the basis of security and usability metrics. Some techniques have good resistance against the various types of attacks. It means they satisfy the security metrics but at the same time they are not easy to use and memorize for all types of users. Also the creation time and login time is more as compare to traditional method. It means not fully satisfy the usability metrics. On the contrary, some techniques are easy to use and memorize but not highly secured. Also a common observation is most of the techniques are not strongly resistant to shoulder surfing attack.

Our proposed technique is easy and resistant to all types of possible attacks specially shoulder surfing to some extent. We have tried here to balance the trade-off between usability and security metrics.

3. Existing System

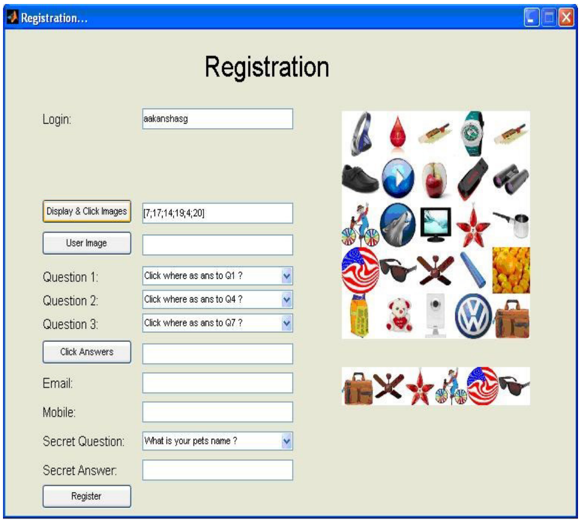
The existing system [17] is a graphical password authentication system. It is a combination of Recognition and Recall based approach. The user authentication is verified in two steps. It works as follows:

3.1 Registration Phase:

1. A user creates his profile by entering personal details and username.
2. Then the 25 images are presented to the user. These images are common to all the users. The user has to select some number of images to set as a password. The user can repeat any image. This is a password for the user's step-I authentication.
3. After this user will choose any image from the stored image database or from the local memory according to his choice.
4. Now he is presented with question set and this image. The user has to select any three questions from this set.
5. To answer a question user has to click on any point on the image. So for three questions there will be three different points. Individual point is called as ROA (Region-Of-Answer). So there are three different ROAs for three different questions. Each ROA is described by a square (center and some tolerance in both X and Y axis).

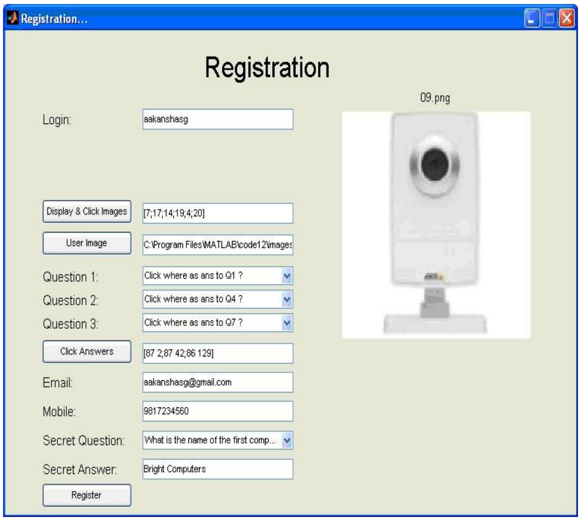
3.2 Login Phase:

1. For step-I authentication user is asked for user name and graphical password. The user has to enter a correct username and for graphical password there should be a correct selection of images in a sequential manner. The order of images within the set will vary at every login.
2. After this, and independent of whether or not it is correct, for step-II authentication, the preselected image and the preselected three questions are shown to the user.
3. Here the order of questions will be random. The user has to click on the correct ROAs according to the order of questions.
4. After the successful entries (selections) in both the steps the user is an authorized user to access the particular system.



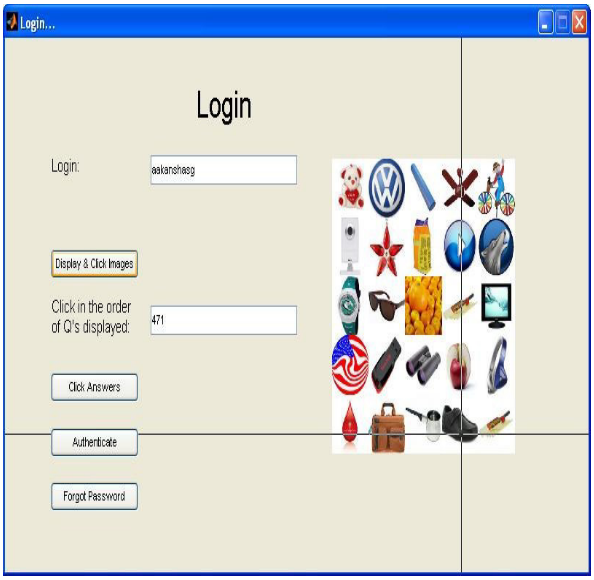
Login: aakanshasg
[7;17;14;19;4;20]
Question 1: Click where as ans to Q1 ?
Question 2: Click where as ans to Q4 ?
Question 3: Click where as ans to Q7 ?
Email:
Mobile:
Secret Question: What is your pets name ?
Secret Answer:

Fig.1 Step-I Registration



Login: aakanshasg
[7;17;14;19;4;20]
C:\Program Files\MATLAB\code12\images
Question 1: Click where as ans to Q1 ?
Question 2: Click where as ans to Q4 ?
Question 3: Click where as ans to Q7 ?
[87 2;87 42;86 129]
Email: aakanshasg@gmail.com
Mobile: 9817234560
Secret Question: What is the name of the first comp...
Secret Answer: Bright Computers

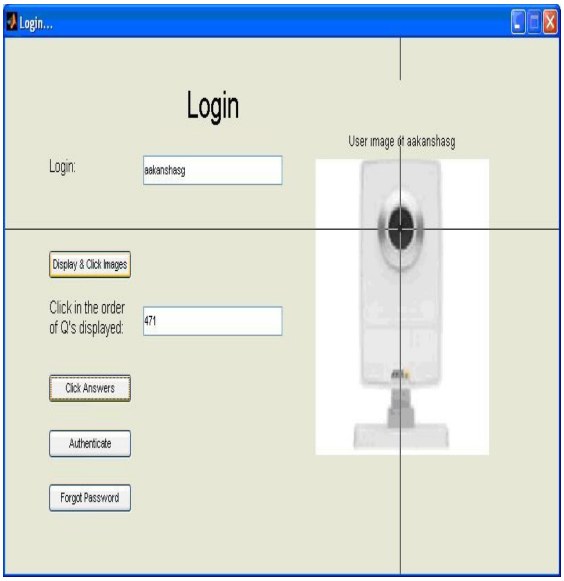
Fig.2 Step-II Registration



Login: aakanshasg

Click in the order of Q's displayed: 471

Fig.3 Step-I Login



Login: aakanshasg

Click in the order of Q's displayed: 471

Fig.4 Step-II Login

4. Proposed System

The proposed system is a modified version of existing system to overcome the limitations of it. It has also two phases.

4.1 Registration Phase:

1. The user enters the username.
2. Then 25 images are shown to the user. The user has to select some number of images to set as a password. This password is called as a secret pass. The minimum number of images in the secret pass should be 6. Also the secret pass should contain even number of images to form the pairs of images. A session password is generated based on this secret pass. This is a password for user’s step-I authentication. This secret pass and session password are the modifications in our system to make the system strongly secure. The images selected by the user are displayed in the panel, below the grid of images in a sequential manner so that selected images can be easily remembered by the user in a sequence. This selected images panel is an addition in our proposed system so that user can confirm the image selections according to his choice. It will disappear after 5 seconds. This makes the system secure as well as user friendly. It is shown in Fig 1.
3. After this user will select any picture from the image database or from the local memory.
4. Then the user is presented with this picture and question set. The user has to select any three questions from the set.
5. As an answer of questions user has to click on any point on the image. So for three questions there will be three different points. Individual point is called as ROA. So there are three different ROAs (Region of Answers) for three different questions. These three different ROAs is the step-II password. It is shown in Fig.2.
6. Also the email-id, mobile number, one secret question from the question set and its related secret answer should be registered by the user during registration. These are the further additions to our proposed system and are shown in Fig 2. These additions will be used when user forgets the password; it will be mailed to user’s registered mail –id by proving his authenticity by answering the secret question correctly.

4.2 Login Phase:

1. For step-I login which is based on recognition based approach user is asked for username. After entering the correct username the user has to enter the graphical password. For this, user is presented with a grid of 25 images, randomly placed on the grid. The image positions will change at every login. The user has to enter the session password depending upon this secret pass. The user has to form the pairs of images in his secret pass. The 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 the session password. For example, during registration, in secret pass suppose first image is bag and second image is fan so during login, first intersection image in session password is shoe. This is shown in Fig.3. In this way it is repeated for all pairs of secret pass. The intersection images in the session password will vary at every login. This makes our system strongly secure. Thus it is very difficult for any imposter to guess or crack this step-I password.
2. Only after successful identifications in step-I, the user can go for step-II login which is based on cued recall based approach. The preselected image and only preselected question numbers instead of whole questions are shown to the user. Both are clues to recall a password.
3. Here the order of question numbers will be random. All the three question numbers are shown as a single three digit number in a text box i.e. 471 as shown in Fig 4. This is a modification in the proposed system for more security. The user has to select the correct ROAs (center and some tolerance in both X and Y axis) according to the order of question numbers. Here only three question numbers are shown to the user as a single three digit number and also its order randomizes at every login. So it is very difficult for attacker to remember step-II password easily.
4. After successful selections in step-II, user is an authorized user to access the system.

Thus step-I and step-II passwords are difficult to guess or crack by attacker, but easy to remember for user. So our proposed system is strongly secure as well as user friendly.

5. Analysis of the System

A proposed system provides a strong security against brute force and guessing attacks as it has a good combination of two types of graphical passwords. It is difficult to guess the password system by a person or by a computer by trying millions of possibilities. It has a very large password space.

For step-I authentication the password space is calculated as:

The number of possible passwords, out of 25 images taken 2 images at a time with minimum three clicks will be:

$$3 * (25\ C\ 2) = \frac{(3 * 25!)}{(2! * 23!)} = 900\ Passwords \qquad (1)$$

However, the above figure is without random shuffling and the random shuffling causes the passwords possible to be:

$$P_1 = 900 * 25! = 1.39*10^{28} > 10^{28}\ Passwords. \qquad (2)$$

For step-II authentication the password space is calculated as:

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

So the password space is:

$$P_2 = \sum_{i=1}^{q} (i! \times [\frac{X \times Y}{z^2}]^{i}) \qquad (3)$$

E.g. Consider the size of the image is 100 × 100; the maximum numbers of questions selected are 3 and suppose the size of the click area (ROA) is 10 × 10, So P_2=6020100.

So available password space by combining two steps is:

$$P = P_1 \times P_2 \tag{4}$$

$$P=(1.39 * 10^{28}) \times 6020100 = 8.367939e+34 \tag{5}$$

Thus scheme has a very large password space so provides a strong security against brute force attack.

It is observed that most of the graphical passwords are vulnerable to shoulder surfing attack but our system provides strong security against it also.

In step-I authentication, the set of 25 images are shown to the user. The size of every image is a thumbnail size. At every login the position of images will vary. So the intersection images which are used as a session password will also vary.

In step-II authentication, the order of question numbers will vary at every login and the all question numbers are displayed as a single three digit number. Thus it is very difficult for any person to guess or crack both step-I and step-II passwords by observing both the passwords at once. Also because of the randomization of password in both the steps the attacker can get confused if he is trying to memorize the password details. In this way our system is strongly resistant to shoulder surfing attack.

Also if any user forgets the password, it is mailed to user's registered email-id by proving authenticity of the user. This feature also adds strong security to our system. If any unauthorized user is trying to access the system, it is impossible for him to get the step-I and step-II passwords. So attacker may go for forget password option to view the password details. But here he has to answer the secret question correctly which is again impossible for him. But this feature is very useful for authorized user to get the forget password details easily.

Thus our system is strongly secure as well as easy to use.

6. Conclusion and Future Scope

Our 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 our 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 our 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. So user can get the system updates although he is offline.

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

References

1. Renaud. "Evaluating authentication mechanisms". In L. Cranor and S. Garnkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6, pp.103-128. O'Reilly Media, 2005.
2. D. Florencio and C. Herley. "A large-scale study of WWW password habits". In 16th ACM International World Wide Web Conference (WWW), May 2007.
3. Xiaoyuan Suo, Ying Zhu, G.Scott. Owen, "Graphical Passwords: A Survey", Department of Computer Science Georgia State University.
4. Kirkpatrick. "An experimental study of memory". *Psychological Review*, 1:602-609, 1894.
5. 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.
6. A. Paivio, T. Rogers, and P. C. Smythe. "Why are pictures easier to recall than words?" *Psychonomic Science*, 11(4):137-138, 1968.
7. R. Shepard. "Recognition memory for words, sentences,and pictures". *Journal of Verbal Learning and VerbalBehavior*, 6:156-163, 1967.

8. W. A. Jansen, "Authenticating Mobile Device Users Through Image Selection," in Data Security, 2004.
9. "ImagePass - Designing Graphical Authentication for Security" Martin Mihajlov E- business Department Faculty of Economics Borka Jerman-Blazi Jožef Stefan Institute Ljubljana, Marko Ilievski Seavus Group 2011.
10. Haichang Gao, Xiyang Liu, Ruyi Dai, "Design and Analysis of a Graphical Password Scheme", International Conference on Innovative Computing, Information and Control (ICICIC), 2009, pp. 675 – 678.
11. Christopher Varenhorst" Passdoodles; a Lightweight Authentication Method ", Massachusetts Institute of Technology, Research Science Institute, July 27, 2004.
12. Jermyn Ian, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin," The design and analysis of graphical passwords", Proceedings of the Eighth USENIX Security Symposium. August 23-26 1999. USENIX Association 1–14, 1999.
13. A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.
14. G. E. Blonder. Graphical passwords. United States Patent 5559961, 1996.
15. Susan Wiedenbeck, Jim Waters, Jean - Camille Birget and Alex Brodskiy, Nasir Memon. PassPoints,"Design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, 63(1-2): 102-127, July 2005.
16. Passlogix,http://www.passlogix.com,Accessed on February 2007.
17. "A New Graphical Password: Combination of Recall & Recognition Based Approach",Md. Asraful Haque, Babbar Imam World Academy of Science Engineering and Technology International Journal of Computer, Information, Systems and Control Engineering Vol: 8 No: 2, 2014.