International Journal of Knowledge Engineering
ISSN: 0976-5816 & E-ISSN: 0976-5824, Volume 3, Issue 2, 2012, pp.-197-201.
Available online at http://www.bioinfopublication.org/jouarchive.php?opt=&jouid=BPJ0000230

AUTHENTICATION SCHEME RESISTANT TO SHOULDER SURFING ATTACK USING IMAGE RETRIEVAL

THORAWADE M.B. AND PATIL S.M.*

[1]MGMCET, Kamothe, Navi Mumbai-410209, MS, India.
[2]BVCOE, Belpada, Navi Mumbai-400 614, MS, India.
*Corresponding Author: Email- smpatil2k@gmail.com

Received: October 25, 2012; Accepted: November 06, 2012

Abstract- A secured authentication system should be incorporated in order to protect secret information from sensitive and various applications. The vulnerabilities of textual passwords are well known, such as short passwords are easy to remember, which makes the passwords vulnerable for attackers to break and some passwords which cannot be easily guessed are often difficult to remember. Shoulder surfing attack refers to using direct observation techniques, such as looking over someone's shoulder to get some information such as password, etc. Hence an alternative solution to text based authentication is image based authentication. However image based authentication is more vulnerable to shoulder surfing attack. In this paper, we propose an authentication scheme resistant to shoulder surfing attack using Image Retrieval. It seamlessly integrates both textual based and image based authentication schemes hence making more secure authentication. Using Image Retrieval user can choose their own choice of image as pass images and can increase password space. We have also discussed their effect on usability and security, which provides resistance to shoulder surfing attack.

Keywords- Shoulder surfing, authentication, image retrieval system, graphical authentication

Citation: Thorawade M.B. and Patil S.M. (2012) Authentication Scheme Resistant to Shoulder Surfing Attack using Image Retrieval. International Journal of Knowledge Engineering, ISSN: 0976-5816 & E-ISSN: 0976-5824, Volume 3, Issue 2, pp.-197-201.

Introduction

Short passwords are easy to remember hence some users tend to use short passwords [1]. Unfortunately, these passwords can also be easily guessed or broken. One of the main problems of textual based password is difficulty of remembering it. Passwords that are hard to guess or break are often hard to remember. Since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts [2, 3]. Hence an alternative authentication method, such as graphical password scheme is used which overcome some problems with traditional username password authentication.

Graphical password schemes have been proposed as a possible alternative to text-based schemes, the psychological studies which supports the fact that humans can remember pictures better than text [4]. Pictures are generally easier to be remembered or recognized than text. Input devices such as mouse, stylus and touch screen that permit make the appearance of graphical user technique possible. Graphical passwords are applied to workstations, web login applications, TM machines and mobile devices.

Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is effective in public places because standing near someone and watch them entering a PIN number at ATM machine is nearly very easy. This attack is also possible at long distance

using binoculars or vision enhancing devices like miniature closed circuit cameras which can be concealed in ceilings, walls or fixtures to observe data entry. The users have been more prone to password thefts because of such kind of sneaking. To prevent shoulder surfing attack it is advised to shield paperwork or the keypad from view by using one's body or cupping ones hand.

Current authentication methods can be divided into:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication
- Association Based Authentication

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

Biometric based authentication techniques are fingerprints, iris scan, or facial recognition. This type of technique provides the

highest level of security. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable.

Knowledge based techniques include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, the user passes the authentication by recognizing and identifying the images from a set of images presented to user which is selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

Using Image based authentication (IBA) in JPEG committee [5], which rests on human cognitive ability of association based memorization. It uses a classic mnemonic strategy called Method of Loci. It also uses recall based technique.

Literature Survey

Recognition Based Techniques

In this technique the user passes the authentication by recognizing and identifying the images from a set of images presented to user which is selected during the registration stage. Haichang Gao, et al [6] proposes a novel graphical password scheme ColorLogin.ColorLogin uses background colour, in which multiple colours are used to confuse the peepers, by decreasing complexity for legitimate users. ColorLogin uses a recognition-based graphical password scheme, choosing multiple images as password icons or pass-icons. It is designed as a Windows XP login authentication scheme which can be used in logging into the system or unlocking the screen.

Zhongje Ren, et al [7] propose a shoulder surfing resistant scheme which has desirable Usability for PDAs (Personal Digital Assistance).It uses Story and DAS (Draw A secret) Method. In this scheme it requires users to draw a secret curve across their password images orderly rather than clicking directly on them. The drawing input trick along with the complementary measures, such as erasing the drawing trace, displaying degraded images, and starting and ending with randomly designated images provide a good resistance to shoulder surfing. This shoulder-surfing resistant scheme is recognition based technique. It suggests users to draw a curve across password images (pass images) in order instead of direct input click. The curve contains both pass-images and decoys which guards against shoulder-surfing attacks. Using a drawing input method, scheme is designed to empower users to log in their mobile devices quickly.

Using a game-like approach, CHC is designed to motivate the users to log in quickly and accurately [8].In this scheme the icons are displayed using only the image without text. The user chooses several icons from the portfolio to be his or her pass-icons to create a password. When the login starts, the user must visually locate three or more of his or her pass-icons. In next step the user is to mentally create the convex hull formed by those pass-icons. The area encompassed by the edges joining a set of three or more points is a convex hull. In CHC the pass-icons serve as the points, and the edges are lines visualized in the user's mind. CHC is based on several rounds of challenge-response authentication.

Recall Based Techniques

Using recall based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. In recall based there are two types of techniques:

Association Based

Zhi li, et al [9] proposes a scheme based on the human cognitive ability of association based memorization. It is based on the principle of zero knowledge proof protocol and reduce shoulder surfing attack without adding any complexity in authentication procedure. In this authentication scheme, two levels of association is created ie association between locus and the object, and the association between the object and its colour.

Repeat a Sequence of Actions

Passlogix [10] has developed a graphical password system on Recall based technique. In this technique, for authentication users must click on various items in the image in the correct sequence. To detect whether an item is clicked by mouse invisible boundaries are defined for each item.

Proposed Scheme

The proposed shoulder surfing resistant scheme can be considered as improvement of S3PAS [11] scheme.S3PAS scheme uses a set of all alphanumeric characters just like conventional textual characters. Hence as the largest set of available passwords icons are limited to the set of all the printable characters (|T| = 94), where T is the set of all printable characters in textual password system. To enlarge the password space T* and make the password easy to remember, we introduce the images as password icons instead of all printable characters. As a result, the password space T* is very much enlarged, which can be used in high capability system to provide high level security. Our proposed system uses content based image retrieval system. [Fig-1] shows a query Image by which we can retrieve images depending on color of Query image as shown in [Fig-2].

We proposed a two stage authentication shown in [Fig-3].

Conventional Authentication

In first stage, authentication is done using Textual Password Authentication. In this step the user as usual enters a username and textual password.

Fig. 1- Query Image

Fig. 2- Retrieved Images

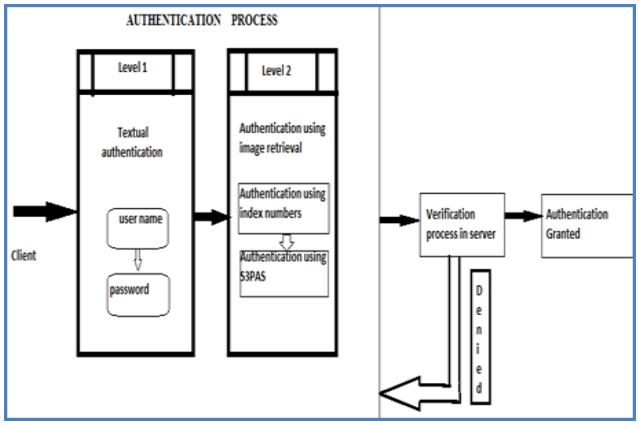

Fig. 3- Authentication process using Image retrieval Flow diagram

Authentication using Image Retrieval Technique.

Our system uses Haar Wavelet transform using Color [12] and edge detection for Image retrieval. We have also used K-means clustering algorithm and Euclidean distance to achieve better results for image Retrieval. The images used are of jpg format with 700 images of dataset.

In this authentication is done by entering index numbers provided to images, using secured authentication protocol system using images [13]. This is an Image-based authentication system based on the premise that 'humans are good at identifying, remembering and recollecting graphical image patterns than text patterns'. Here user has to enter the index number provided at the images. While entering index numbers in the password area it will be hidden and bullet marks will be displayed. For example, if the client chooses images 600.jpg, 601.jpg and 675.jpg then their corresponding index numbers 59, 09 and 40 should be entered in a selected order. While confirming password images index numbers were shuffled, so user has to re-enter the password by giving different index numbers according to the images chosen. Here both image patterns and index numbers are represented as dynamic arrangements in every login attempt. Due to this setup no one would be able to read or guess the mechanism involved. For every authentication the images were shuffled and index numbers were varied and shuffled. It is represented in [Fig-4].

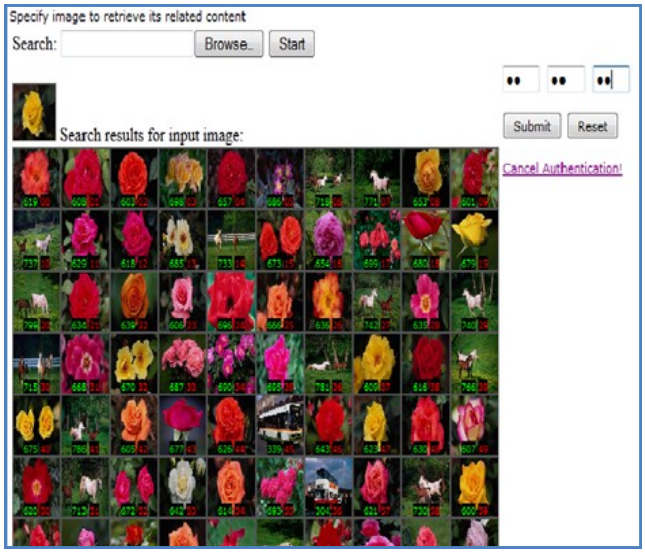

Fig. 4- Login Interface for Image icons with index numbers

Using this mapping mechanism the shuffling process of images and index numbers are generated. The images are validated only by using the hidden characters and index numbers which reduce the time complexity of comparing the images. The image positions are generated using permutation sequences. For n images n! Sequences were generated and it will be used randomly for every attempt of registration.

Authentication using S3PAS Scheme

In this scheme authentication is done by selecting the images from the pass images which is considered as a triangle. To login, the user must find all his/her original pass images in the retrieved images and then make some clicks inside the invisible triangles which are called pass-triangles created by original 3 pass images following a certain click rule. Therefore, the final inputs are several session pass clicks. These session pass clicks is a users session pass images. Users choose their original pass images when creating their accounts. In every login process, users input different session pass images so that they can protect their original pass image from releasing. For example suppose the user has entered pass images as 400.jpg, 401.jpg, 402.jpg, 403.jpg during login process. As the user has entered 4 pass images, hence user has to click four times correctly in the right sequence to be authenticated. The four combinations of pass images in order are "400.jpg, 401.jpg,402.jpg", "401.jpg, 402.jpg, 403.jpg","402.jpg, 403.jpg,400.jpg"and "403.jpg, 400.jpg, 401.jpg".Hence to login the user has to click in between:

- Invisible triangle formed by "400.jpg, 401.jpg, 402.jpg" i.e. 471.jpg with index number 35.
- Invisible triangle formed by "401.jpg, 402.jpg, 403.jpg"ie 463.jpg with index number 32.
- Invisible triangle formed by"402.jpg, 403.jpg, 400.jpg" i.e. 482.jpg with index number 36
- Invisible triangle formed by"403.jpg, 400.jpg, 401.jpg"ie 453.jpg with index number 43

In this example, the users original pass images are 400.jpg, 401.jpg, 402.jpg, 403.jpg and session pass images are 471.jpg, 463.jpg, 482.jpg, 453.jpg where user has to click four times inside the invisible pass images in sequence to be authenticated.

For authentication the user should click inside the triangle area formed by pass images during registration stage, shown in [Fig-5].

Analysis

Security

System security largely depends on having sufficiently large password space; the main defence against brute force search. Graphical passwords are less vulnerable to brute force search. Text-based passwords 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 our scheme as it uses 100 images in a single login interface it has sufficiently large password space. As large password space using images our system is less vulnerable to brute force search attack. In first level of authentication as it uses three pass images from 100 images to enter respective index number and in second level it uses S3PAS which uses n password images, where n is length of pass images from 100 images as shown in login interface [Fig-4] and [Fig-5].

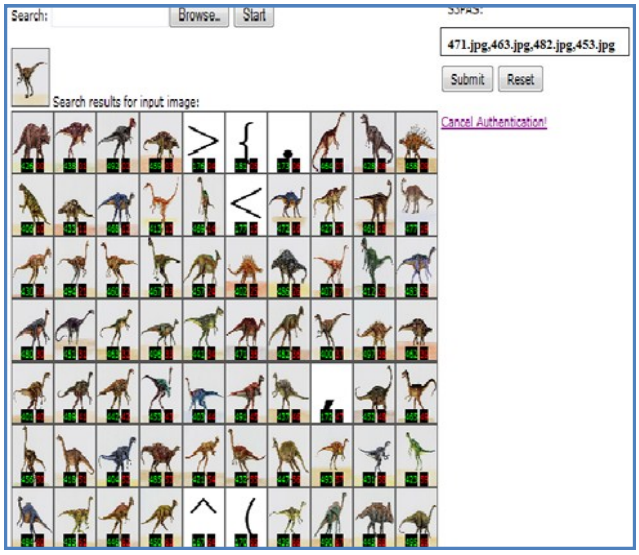

Fig. 5- Login Interface for Authentication using S3PAS Scheme using images.

Dictionary Attacks

Image based passwords are less vulnerable to dictionary attacks than text-based passwords.

Social Engineering

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. 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. Hence it is more difficult to break graphical passwords using the traditional attack methods like brute force search, dictionary attack, and shoulder surfing attack.

Usability

Graphical passwords are easier to remember than text strings. Password registration and log-in process take too long in recognition-based approaches. Users may find the authentication process long and tedious. As most of the users are not familiar with the graphical passwords, they often find graphical passwords less convenient than text based passwords.

Storage and Communication

Graphical passwords require much more storage space than text based passwords. Tens of thousands of pictures may have to be maintained in a centralized database. Network transfer delay is also a concern for graphical passwords, especially for recognition-based techniques in which a large number of pictures may need to be displayed for each round of verification.

Reliability

The major design issue for recall-based methods is the reliability and accuracy of user input recognition. In this type of method, the error tolerances have to be set carefully – overly high tolerances may lead to many false positives while overly low tolerances may lead to many false negatives. In addition, the more error tolerant the program, the more vulnerable it is to attacks.

Shoulder Surfing

Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. In our system, the attacker cannot identify the three pass images as well as their corresponding index numbers even though the pass images are visible and index numbers corresponding to these pass images change for every session. *Hence i*t is not possible to know the password as the observer cannot predict the actual index numbers of the pass images. Using S3PAS scheme it is not possible for an attacker to recognize the pass images as the user can click on any image inside the triangle formed by pass image and because of the generation of session passwords for every login, these techniques are not vulnerable to shoulder surfing.

Conclusion

We proposed an authentication scheme resistant to shoulder surfing attack using Image Retrieval. As Image based passwords are more difficult to break using the traditional attack methods such as brute force search, dictionary attack and resistant to shoulder surfing it is highly secure. Image based passwords are better in memorizing than textual passwords. As our scheme is more secure by using both conventional and image based authentication with two levels of security it reduces shoulder surfing attack.However, the major issue in proposed system includes longer login process. Hence more research has to be carried out as to achieve higher levels of maturity and usefulness.

References

[1] Adams A. and Sasse M.A. (1999) *Communications of the ACM*, 42, 41-46.

[2] Dhamija R. and Perrig A. (2000) 9*th USENIX Security Symposium*.

[3] Kotadia M. (2005) *ZDNet,* Australia.

[4] Shepard R.N. (1967) *Journal of Verbal Learning and Verbal Behavior*, 6, 156-163.

[5] Ginesu G., Giusto D., Onali T. (2004) *JTC,* 1/SC 29/WG1.

[6] Davis D., Monrose F. and Reiter M.K. (2004)13*th Usenix Security Symposium*, San Diego, CA.

[7] Sobrado L. and Birget J.C. (2002) *The Rutgers Scholar*, 4.

[8] Zhi Li, Qibin Sun, Yong Lian and Giusto D.D. (2005) *IEEE International Conference on Multimedia and Expo*(ICME).

[9] Haichang Gao, Xiyang Liu, Sidong Wang, Honggang Liu and Ruyi Dai (2009) *Fourth International Conference on Innovative Computing, Information and Control*, Kaohsiung, Taiwan.

[10] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu (2010) *International Conference on CyberWorlds*, Singapore.

[11] Huanyu Zhao and Xiaolin Li (2007) 21*st IEEE International Conference on Advanced Information Networking and Applications Workshops*.

[12] Latha Y.M., Jinaga B.C., Reddy V.S.K. (2007) *International Journal of Computer Science and Network Security*, 7(12).

[13] Arumugam G., Sujatha R. (2010) *International Journal of Computer Science and Information Security*, 8(8).