International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:2, 2014

A New Graphical Password: Combination of Recall & Recognition Based Approach

Md. Asraful Haque, Babbar Imam

***Abstract*—**Information Security is the most describing problem in present times. To cop up with the security of the information, the passwords were introduced. The alphanumeric passwords are the most popular authentication method and still used up to now. However, text based passwords suffer from various drawbacks such as they are easy to crack through dictionary attacks, brute force attacks, keylogger, social engineering etc. Graphical Password is a good replacement for text password. Psychological studies say that human can remember pictures better than text. So this is the fact that graphical passwords are easy to remember. But at the same time due to this reason most of the graphical passwords are prone to shoulder surfing. In this paper, we have suggested a shoulder-surfing resistant graphical password authentication method. The system is a combination of recognition and pure recall based techniques. Proposed scheme can be useful for smart hand held devices (like smart phones i.e. PDAs, iPod, iPhone, etc) which are more handy and convenient to use than traditional desktop computer systems.

***Keywords*—**Authentication, Graphical Password, Text Password, Information Security, Shoulder-surfing.

I. Introduction

PASSWORDS provide security mechanism for authentication and protection services against unwanted access to resources. The most common approach for authentication is alphanumeric passwords. However, it is well-known that text passwords are insecure for a variety of reasons. Text password is simply a string of letters and digits. Although almost any string can serve as a password, these passwords only offer good security as long as they are complicated enough so that they cannot be deduced or guessed. Alphanumerical passwords are versatile and easy to implement and use. They are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostor [1]. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks [2], [3]. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft [4]. Text passwords can be stolen by malicious software (e.g., keystroke loggers) when being entered from keyboards.

Phishing is another serious threat to text passwords, by which, a user could be persuaded to visit a forged website and enter their passwords. So a big necessity to have a strong authentication method is needed to secure all our application as much as possible. To overcome the shortcomings of text-based passwords, graphical passwords have been proposed. In most of the schemes, graphical password employs graphical presentations such as icons, human faces or custom images to create a password. Human brains can process graphical images easily. Graphical passwords claim to be superior to the text based passwords due to this human characteristic. These methods assume if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based password and therefore it is virtually more resistance to attacks such as dictionary attacks. Graphical password techniques can be classified into two categories; recognition-based and recall-based. In recognition-based systems, a series of images are presented to the user and a successful authentication requires correct images being clicked in a right order. In recall-based systems, the user is asked to reproduce something that he or she created or selected earlier during the registration. The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. But the shoulder-surfing is an eminent problem that has been difficult to overcome in graphical passwords. Shoulder surfing is a direct observation technique, such as looking over someone's shoulder, to get passwords, PINs and other sensitive personal information. When a user enters information using a keyboard, mouse, touch screen or any traditional input device, a malicious observer may be able to acquire the user's password credentials. In this paper, we have tried to present a shoulder surfing resistant graphical password scheme. The structure of our paper is organized as follows. Section II provides an overview of some existing graphical password techniques. Section III explains our new proposed scheme. Section IV analyses the scheme in different dimensions. Section V concludes the paper with some remarks.

II. Related Work

The basic need for graphical password is that graphical passwords are expected to be easier to recall, less likely to be written down and have the potential to provide a richer symbol space than text based password. Researchers are continually introducing new ideas, concepts, and features in the field of graphical authentication. There are already many approaches have been proposed in present times. Blonder gave the initial idea of graphical password in 1996. In his scheme, a user is presented with one predetermined image on a visual display

Md. A. Haque is with the Computer Engineering Department, Aligarh Muslim University, U.P.-202002, India (e-mail: asrafb4u@gmail.com).
B. Imam is with the Tata Consultancy Services, Kolkata, India (e-mail: babbarimam5@gmail.com).

and required to select one or more predetermined positions on the displayed image in a particular order to access the restricted resource [5]. The major drawback of this scheme is that users cannot click arbitrarily on the background. The memorable password space was not studied by the author either. Wiedenbeck et al. [6] proposed PassPoint method in which they 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. Sonia Chiasson et al. [7] proposed Cued Click Points (CCP), a cued-recall graphical password technique. A password consists of one click-point per image for a sequence of 5 images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. A major usability improvement over PassPoints is the fact that legitimate users get immediate feedback about an error when trying to log in. When they see an incorrect image, they know that the latest click-point was incorrect and can immediately cancel this attempt and try again from the beginning. Few grid based schemes are proposed which uses recall method. Jermyn et al. [8] proposed a technique called "Draw A Secret" (DAS) where a user draws the password on a 2D grid. The coordinates of this drawing on the grid are stored in order. During authentication user must redraw the picture. The user is authenticated if the drawing touches the grid in the same order. The major drawback of DAS is that diagonal lines are difficult to draw and difficulties might arise when the user chooses a drawing that contains strokes that pass too close to a grid-line. Users have to draw their input sufficiently away from the grid lines and intersections in order to enter the password correctly. If a user draws a password close to the grid lines or intersections, the scheme may not distinguish which cell the user is choosing. Syukri et al. [9] proposed a system where authentication is conducted by having the user drawing his/her signature using a mouse. The biggest advantage of this approach is that there is no need to memorize one's signature and signatures are hard to fake. However, not everybody is familiar with using mouse as a writing device; the signature can therefore be hard to drawn. Dhamija and Perrig [10] proposed a graphical authentication scheme in which the user selects certain number of images from a set of random pictures during registration. Later user has to identify the pre-selected images for authentication. The users are presented a set of pictures on the interface, some of them taken from their portfolio, and some images selected randomly. For successful authentication, users have to select 'their' pictures amongst the distracters. Passface is a technique developed by Real User Corporation based on the assumption that people can recall human faces easier than other pictures [11]. The basic idea is same as Dhamija and Perrig method. Here the user is asked to choose four images of human faces from a face database as their password.

These techniques have the potential to fill the gaps left between traditional authentication techniques, including trade-offs between security levels, expense and error tolerance. But unfortunately there is a common weakness in the above graphical password schemes: They are all vulnerable to shoulder-surfing attacks. To address this issue, Sobrado and Birget developed a graphical password technique [12]. In their scheme, the system first displays a number of 3 pass-objects (pre-selected by a user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the triangle formed by the 3 pass-objects. Huanyu Zhao et al. [13] proposed a Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS). In this scheme, user is provided with the login-image which consists of 93 printable characters. To login, the user must find all his/her original pass-characters in that image and then make some clicks inside the invisible triangles which are called pass-triangles. The pass-triangles are created by 3 original pass-characters following a certain click-rule. In this scheme, user pass-character lies inside the pass-triangle. If the user password length is k then he has to click k-times inside the invisible pass-triangles. In S3PAS if the size of every pass-triangle area is too large, attackers are able to click inside the right areas with higher probabilities. Haichang Gao et al. [14] has proposed a recognition-based graphical password scheme ColorLogin. It is implemented in an interesting game way to weaken the boring feelings of the graphical authentication. ColorLogin uses background color, a method not previously considered, to decrease login time greatly. Multiple colors are used to confuse the peepers, while not burdening the legitimate users. The scheme is resistant to shoulder surfing attack but password space is smaller than text-based passwords. Man et al. [15] proposed another shoulder-surfing resistant algorithm in which 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 and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object. However, these methods force the user to memorize too many text strings, and their shoulder-surfing resistant property is not strong either. In real scenario, these approaches are under-utilized as the authentications are usually complex and boring for users.

III. Our Proposal

The graphical password is not widely deployed in real systems due to the problem of shoulder surfing. The other vulnerabilities of graphical passwords are still not fully understood. In this paper, we have suggested a shoulder-surfing resistant graphical password authentication method. The system is a combination of recognition and pure recall based techniques. User authentication has been verified in two steps to increase the security. The proposed authentication system works as follows.

A. Registration Phase

1. A user creates his profile by entering personal details and username.
2. Then he is presented with a set of 25 images as shown in Fig. 1. This is the common image-set for all users. The user has to select any number of images from this set. Even he may choose a single image more than once. This selection will act as the password of his first step of authentication.

Fig. 1 Image-set for registration

3. Next he will choose any picture from the stored image database or from the local memory at his own choice.
4. Now he is presented with a set of questions and this image. The user has to select any three questions from the set.
5. To answer each question he will click on any point of the image. So for three questions there will be three region-of-answers (ROA) within the image and each question will be associated with an ROA. Each ROA is described by a square (center and some tolerance in both X and Y axis).

B. Login Phase

1. In step-1, a user is asked for his user name and graphical password (correct selection of images in a correct sequence). The order of images within the set will be random at every login time. This authentication step is shown in Fig. 2.

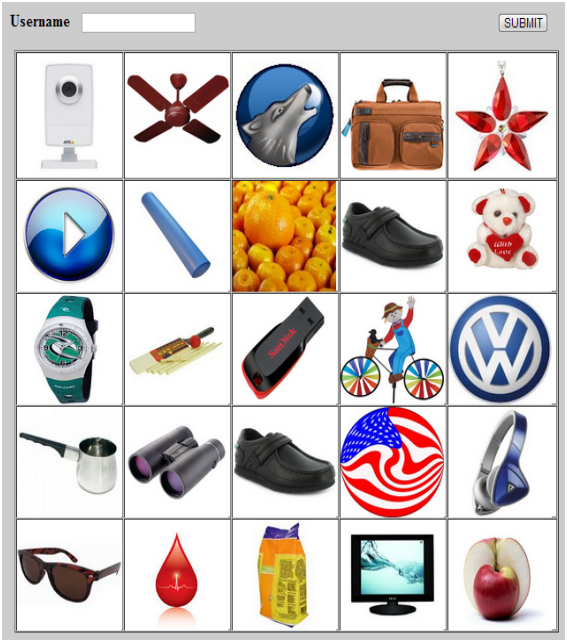

Fig. 2 Step-1 Authentication

2. After supplying this, and independent of whether or not it is correct, in step-2 authentication, the user is presented with the set of three questions and the pre-selected image.
3. 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 in both steps the user is allowed to access his account. The screenshot of the step-2 authentication is shown in Fig. 3.

Fig. 3 Step-2 Authentication

IV. Analysis of the Scheme

A new password scheme should provide good combination of passwords which are strong enough against guessing and brute-force attacks. The necessary quality of the password depends on how well the password system limits attempts to guess a user's password, whether by a person who knows the user well, or a computer trying millions of possibilities [3]. Password strength directly depends on the password space i.e. maximum possible number of passwords generated by the system. So to analyze any scheme one must calculate its

password space. In our scheme, the password space of step-1 authentication will be

$$R_1 = \sum_{i=1}^{p} 25^i ;$$

p is the maximum no. of images used to form the password. Now consider the step-2 authentication. Let M×N be the size of the image portfolio and q be the maximum number of questions selected in our graphical password verification. For each question, suppose the size of the allowable click-area is n×n. The password space of a randomly selected graphical password conforming to this policy is

$$R_2 = \sum_{j=1}^{q} \left(j! \times [\tfrac{M \times N}{n^2}]^j \right).$$

If we combine these two steps, we will achieve the available password space of our scheme. The available password space is

$$P = R_1 \times R_2.$$

So, the scheme provides a very large password space. Enormous effort is required to carry out a brute force attack against our scheme. It is clear that in our scheme, the step-2 authentication page will be different for each user. Without knowledge of users' image profiles, the phisher does not know what images to present in order to extract a graphical password. Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, our policy provides a solid resistance against shoulder surfing attack. In step-1 authentication, the user is presented with a set of 25 images. Naturally the size of each image will be very small and each login time the order of the images will be random. In step-2 authentication, each time the order of the questions will be random. It is a very difficult task for a person to crack both the step-1 password and as well as all the ROA's by observing user's movement at once. The randomization technique of our scheme is specially deployed to make an imposter confused who is trying to memorize the authentication details from the backside. The scheme can be useful for highly secure systems.

V. Conclusion

We do believe that our design will prove to be more usable and adequately secure for user authentication than existing graphical password methods. The first step of our scheme is a recognition based whereas the next step is a recall based technique. The major design issue for any recall-based method 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. We have assigned an acceptable size to an ROA to minimize the false positives and false negatives. For an actual point (x, y) we allow the user to click any point which has the X-coordinate in between (x-5) to (x+5) and Y-coordinate in between (y-5) to (y+5). It means the length of the side of each ROA square is 10. In addition, the more error tolerant the program, the more vulnerable it is to attacks. Current graphical password techniques are still immature. Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text based passwords. Encryption and transferring over the internet are two vital issues that remain un-discussed among all the works we encountered. Traditional text-based password can be encrypted into a string while transferring, but if pictures are encrypted into a string as well, it then reveals no advantage against text based password. So the question remains to be how to encode the graphical password in reality. The field is new and open for future works. Proposed scheme will provide the following advantages:

1. Easy to use and memorize.
2. Easy to create the password
3. Random nature in authentication phase provides a resistance to the shoulder surfing attacks.
4. It provides sufficient security against brute force and phishing attacks.
5. Password space is very large.
6. It can be implemented in software alone, increasing the potential for large-scale adoption on the Internet.

References

[1] William Stallings and Lawrie Brown, "Computer Security: Principle and Practices." Pearson Education, 2008.
[2] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," 21st Annual Computer Security Applications Conference (ASCSAC 2005). Tucson, 2005.
[3] Md. Asraful Haque, Babbar Imam, Nesar Ahmad, "2-Round Hybrid Password Scheme", International Journal of Computer Engineering and Technology (IJCET), Vol. 3, Issue 2, July-September (2012), page. 579-587.
[4] D.Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.
[5] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent-5559961, Ed. United States, 1996.
[6] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon, "Passpoints: design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, 63:102–127, July 2005.
[7] Sonia Chiasson, P.C. Van Oorschot, and Robert Biddle, "Graphical Password Authentication Using Cued Click Points", 12th European Symposium on Research in Computer Security (ESORICS), 2007, pp. 359-374
[8] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, "The design and analysis of graphical passwords", Proceedings of the 8th USENIX Security Symposium Washington, D.C., USA, August 23–26, 1999
[9] 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.
[10] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.
[11] Real User Corporation, "How the Passface System Works", 2005.
[12] L. Sobrado and J.-C. Birget, "Graphical Passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
[13] Huanyu Zhao and Xiaolin Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", 21st

International Conference on Advanced Information Networking and Applications Workshops, AINAW '07. Page(s): 467 – 472.
[14] 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.
[15] S.Man, D. Hong, and M. Mathews, "A Shouldersurfing Resistant Graphical Password Scheme", In Proceedings of International Conference on Security and Management, Las Vegas, NV, 2003.

Md. Asraful Haque was born in 1985 in West Bengal, India. He received his Master degree in Computer Science and Engineering (Specialization-Software Engineering) from Aligarh Muslim University. Presently he is an Assistant Professor (Ad-hoc basis) in Aligarh Muslim University. He has near about of five years of teaching experience. His area of interests includes Software engineering, Operating Systems, Data Structure, Image Processing and Password Security. He is a reviewer of several reputed journals. He has authored several papers in different international journals and conferences.

Babbar Imam received his M.Tech degree in Computer Science and Engineering from Aligarh Muslim University in 2013. He is presently working in TCS, Kolkata as a software developer. He has two years of teaching experience. His area of interests includes Software engineering, Artificial Intelligence, Image Processing and Password Security.