ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, No 6, June 2013

A Proficient Multilevel Graphical Authentication System

A Aswathy Nair[#1], Theresa Rani Joseph[#2], Jenny Maria Johny[#3]

[#] *Department of Computer Science, St. Joseph's College Of Engineering & Technology*
Palai, Kottayam, Kerala, India

***Abstract*—Text passwords are the most commonly used technique for authentication and have several drawbacks. Graphical passwords provide a promising alternative to traditional alphanumeric passwords due to the fact that humans can remember pictures better than text. In this paper, we propose a simple graphical password authentication system that consists of a sequence of 'n' images and the user have to select the click points associated with one of the 'n' image in correct sequence for successful login. This authentication system employs the user's personal handheld device as the second factor of authentication. With the increasing popularity of handheld devices such as cell phones, our approach can be leveraged by many organizations to overcome threats such as key-loggers, shoulder surfing, weak passwords.**

***Keywords*— Graphical passwords, Authentication, Key-loggers, Shoulder surfing.**

I. INTRODUCTION

Authentication in the computer world refers to the act of confirming the authenticity of the user's digital identity claim. It is a fundamental component in most computer security contexts and provides the basis for access control and user accountability. Current authentication methods are classified as biometric based, token based and knowledge based authentication as in figure1. Biometric based authentication provides more reliable user authentication which uses finger print, iris scan or facial recognition. Token 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 generally require a PIN number which is to be remembered by the user. Knowledge based authentication system can be text based or picture based.

While there are various types of user authentication systems, alphanumerical username/passwords are the most common type of user authentication. They are versatile and easy to implement and use. In the simplest form, a system that requires authentication challenges the user for a secret, typically a pair of username and password. The entry of the correct pair grants access on the system's services or resources.

Two contradictory requirements are to be satisfied by the text passwords. First requirement is that the passwords have to be easily remembered by a user and the second is that have to be hard to guess by the attacker. Easily guessable and/or short text passwords are normally chosen by the user, which are an easy target of dictionary and brute-forced attacks. Enforcing a strong password policy sometimes leads to an opposite effect as a user may tend to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft. Another crucial problem is that users tend to reuse passwords across various websites. Password reuse causes users to lose sensitive information stored in different websites if a hacker compromises one of their passwords. For long time the computer industry has been in a quest for better alternatives but without popular success, still most of our current systems use the alpha numeric password authentication schemes.

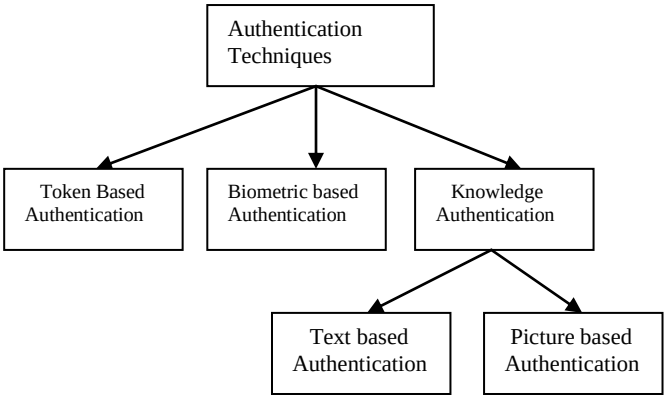

Fig. 1. Classification Of Authentication Technique

To overcome some of the shortcomings of the textual passwords, researchers turned their attention to passwords that utilize graphical objects. Graphical authentication has been proposed as a user-friendly alternative to password generation and authentication. In this approach the user enters the password by clicking on a set of images, specific pixels of an image, or by drawing a pattern in a pre-defined and secret order. Passwords are more likely to be recognized and remembered if they are presented as pictures rather than as words. Thus, graphical password presumably delivers a higher usability compared to text-based password.

Another alternative for alpha numeric password based authentication is the use of password management tools. For each website, strong passwords are automatically generated by this tool, which addresses password reuse and password recall

problems. The advantage is that users only have to remember a master password to access the management tool.

Three-factor authentication is an authentication system which includes all the three mechanisms and depends on what you know (eg: password), what you have (eg: token), and who you are (eg: biometric). To pass the authentication, the user must input a password and provide a pass code generated by the token, and scan her biometric features (e.g., fingerprint or pupil). The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security. Two-factor authentication is more attractive and practical than three-factor authentication, and is based on token based and text based authentication system.

In this paper, we describe a new and more secure graphical password authentication system. The system combines graphical passwords mechanism with a handheld device to form a novel method of multi-factor authentication. This approach includes multiple images and the user need to select click points for each image. In the login phase one among the set of images is provided to the user for marking the click points in the correct order which prevents the shoulder surfing attack. The best feature of this approach is that in case of authentication failure, next image will be displayed only after providing the one time password, which is send by the server to the user's mobile.

II. Related work

Text-based username and password is vulnerable to guessing, dictionary attack, key-loggers, shoulder-surfing and social engineering. As mentioned before, to overcome the shortcomings of text-based password, techniques such as two-factor authentication and graphical password have been employed. In general, Graphical password method is a type of knowledge base authentication system and graphical password schemes can be grouped into three general categories based on the type of cognitive activity required to remember the password: recognition, recall, and cued recall. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Cued recall falls somewhere between these two as it offers a cue which should establish context and trigger the stored memory. Most existing systems are based on recognition.

Bensinger et al. [9] proposed a graphical authentication system on passfaces, which is a best known recognition based system. To create a password, the user chose four images of human faces from a portfolio of faces. To log in the user saw a grid of nine faces, which included one face previously chosen by the user and eight decoy faces. The user had to click anywhere on the known face. This procedure was repeated with different target and decoy faces, for a total of four rounds. If the user choose all four correct faces, he or she successfully logged in. Data from this study suggest that Passfaces are more memorable than alphanumeric passwords. On the other hand, passwords based on image recognition have a serious disadvantage. Only a small number of faces can be displayed on each screen, e.g., in Passfaces nine faces. An attacker has a 1-in-9 chance of guessing this passface. With a few thousand random guesses an attacker would be likely to find the password. To increase security similar to that of 8-character alphanumeric password, 15 or 16 rounds would be required. This could be slow and annoying to the user.

Ahmad et al[2] proposed another implementation of passface, which include the combination of passface and text based passwords. At the time of registration, a graphical password is created by the user by first entering a picture he or she chooses. Then several point-of-interest (POI) regions in the picture is chosen by the user. Each POI is described by a circle (center and radius). For every POI, the user types a word or phrase that would be associated with that POI. If the user does not type any text after selecting a POI, then that POI is associated with an empty string. The user can choose either to enforce the order of selecting POIs (stronger password), or to make the order insignificant. The problem with this method is that the user need to remember both the click points and the text associated with each click points.

Susan et al[11] proposed the Pass-Points graphical password scheme, in which a password consists of sequence of 5 to 8 different click points on a single image and the click points are chosen by the user. The image is displayed on the screen by the system. The image is not secret and has no role other than helping the user remember the click points. Any pixel in the image is a candidate for a click point. Pass-Point comes under click based graphical password scheme. The main disadvantage of this scheme are HOTSPOTS and pattern formation attacks.

Sonia et al[13] proposed Cued Click Points which was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Instead of five click-points on one image, cued click points uses one click-point on five different images. The next image displayed is based on the location of the previously entered click-point. One best feature of Cued Click Point is that the message of authentication failure is displayed after the final click-point, to protect against incremental guessing attacks. But this technique has several disadvantages like false accept (the incorrect click point can be accepted by the system) and false reject (the click-point which is to be correct can be reject by the system).In this system pattern formation attack is reduced but HOTSPOT remains since users are selecting their own click-point.

Man, et al. [3] proposed a 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. The argument is that it is very hard to crack this kind of password even if the whole authentication process is recorded on video because where is no mouse click to give away the pass-object information. However, this method still requires users to memorize the alphanumeric code for each pass-object variant.

Alireza et al[1] introduced the use of personal device in combination with the graphical password. In this approach some hint information is transmitted to the personal device such as mobile phone, to determine the appropriate click points and their order, for each login session. The hint information is transmitted either through direct communication, photographic communication or indirect communications. This approach prevents the user from remembering the click points. But this approach has several disadvantages like shoulder surfing, pattern formation attack etc.

III. Proposed System

In this paper, we present a more secure graphical password mechanism based on the passpoint based technique. Pass point graphical password scheme is the one in which a given image password consists of a sequence of different click points. For password creation user selects any pixel in the image as a click point and for login the user has to enter the same series of clicks in correct sequence within a system defined tolerance square of original click-points. The proposed authentication system consists of a sequence of 'n' images and the user has to select three click points from each image. During login one of the 'n' images will be provided to the user and the user have to select the three click points associated with that image in correct sequence for successful login. This system leverages the user's cellphone and communication service in case of incorrect authentication attempts. This is to prevent incremental guessing attacks. The proposed authentication system includes three phases. We introduce the details of these three phases respectively.

A. *Registration Phase*

For the user to get access to the website and to get privileged to access the services, the first step is to register to the website. The registration phase includes 3 steps. The user after selecting the username is asked to select a set of 'n' images. The image selection can be done either from those chosen by the user or those generated by the system. Next the user have to select a sequence of three click points on each of the 'n' images. In the final phase of registration, user have to submit his/her mobile phone number and install the i-rem software in the cell phone. I-rem software generates a key and exchange. the key with the server after encrypting the key using the server's public key.

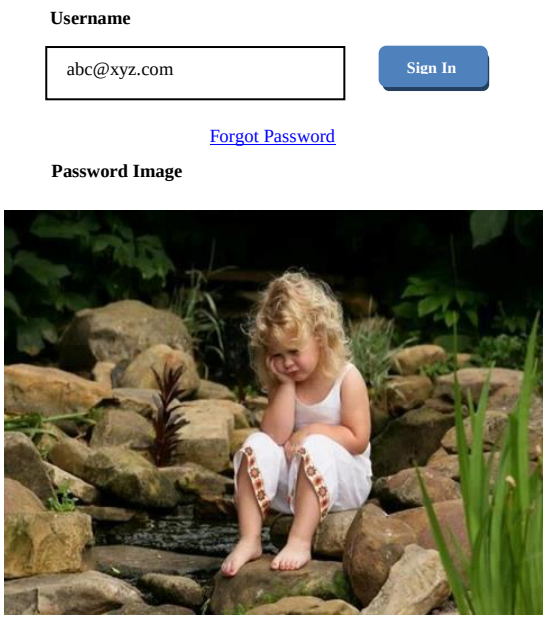

Fig2: Login Phase

B. *Login Phase*

In the login phase, the user submits the username to the website. The username transmitted to the database by the server is used as the key to retrieve the images associated with that user. One image among the 'n' is chosen randomly and is provided to the server. The user is asked to click on the click points associated with that image as shown in figure 2. The user is authenticated if the user selects the correct click points. The incorrect pointing of click points leads to the unsuccessful authentication.

C. *Authentication Failure*

The authentication failure occurs as the result of incorrect marking of the click points. This leads to the generation of a one-time password by the server. The one time password encrypted with the shared key is directed to the i-rem software installed in the user's cellphone as in figure3. The user get access to the decrypted one time password after unlocking of the password protected i-rem software. The decryption is done using the same shared key as that used for encryption by the server. The next image can be retrieved only by providing the one time password generated by the sever for that session. The encryption and decryption can be done using the AES algorithm.

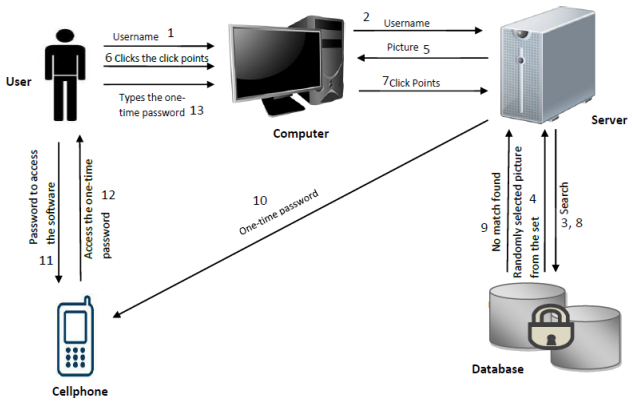

Fig 3: Authentication Failure

The proposed system includes 'n' number of images and each image consists of 3 click points. There is a chance that the user may get confused or forgets the click points. In this case, an option for forgot password is provided. In this option, the server retrieves the image along with its hints from the database. This image with the click points marked as shown in figure4 is encrypted by the server with the shared key and is send to the i-rem software in the user's cellphone. The user can access the decrypted image and its hints by unlocking the software. The password image along with the click points is automatically deleted from the cellphone after a predefined time interval.

Fig 4: Password hint send to mobile

Since the system uses a set of images rather than one and the image set can be chosen from user image collection, hotspot can be eliminated. The login phase of this authentication system, ask the user to mark the click points from one image among the set for each session. Since for each login session different image from set is chosen in a random fashion shoulder surfing and pattern formation attack can be avoided. When the authentication fails due to the incorrect pointing of click points, the next image is displayed only if the user inputs the one time password received in his/her mobile phone, which provides protection from incremental guessing attacks. If an attacker steals a user's cellphone and attempts to log into a website that the victim has visited, he will not succeed, since the i-rem software installed in user mobile is password protected and hence the attacker cannot access the software.

IV. Conclusion

User authentication is a fundamental component in most computer security contexts. In this paper, we proposed a more secure graphical password authentication system. The main reason for adaption of graphical password is that people are better at memorizing graphical passwords than text-based passwords. The system combines graphical password scheme along with a handheld device to form a novel method of multi-factor authentication. This authentication scheme ensures the protection from threats such as key loggers, hotspot, shoulder surfing etc.

References

[1] Alireza Pirayesh Sabzevar and Angelos Stavrou, "Universal Multi-Factor Authentication Using Graphical Passwords," in IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008

[2] Ahmad Almulhem, "A Graphical Password Authentication System," in 978-0-9564263-7/6/$25.00 IEEE, 2011

[3] S. Man, D. Hong, and M. Mathews, "A shoulder-surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003

[4] Birget, J.C., D. Hong, And N. Memon, "Graphical Passwords Based On Robust Discretization" IEEE Trans. Info. Forensics And Security, 1(3), September 2006.

[5] Thorpe, J. and P.C. van Oorschot. Human-Seeded Attacks and Exploiting HotSpots in Graphical Passwords. 16th USENIX Security Symposium, 2007.

[6] Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, 2005, 'An Association-Based Graphical Password Design Resistant to Shoulder Surfing Attack', IEEE International Conference on Multimedia and Expo (ICME).

[7] 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

[8] Surfing Attack', IEEE International Conference on Multimedia and Expo (ICME).

[9] Bensinger, undated, Brostoff and Sasse, "Passfaces: Two Factor Authentication For Enterprise" Real User Corporation, 2001.

[10] Blonder, G.E, "Graphical Passwords", United States Patent 5,559,961, 1996.

[11] Susan Wiedenbeck,Jim Waters, Jean-Camille Birget,Alex Brodskiy, Nasir Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system", Int. J. Human-Computer Studies 63 (102–127 ,2005.

[12] G.Agarwal, S.Singh, R.S.Sukhla "Security Analysis Of Graphical Passwords Over The Alphanumeric Passwords" Int. J. Pure Appl. Sci. Technol., 1(2), pp. 60-66,2010

[13] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, "Graphical Password Authentication Using Cued Click Points", J.Biskup and J. Lopez (Eds.): ESORICS 2007, LNCS 4734, pp.359-374, 2007.