World Applied Sciences Journal 32 (10): 2140-2145, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.32.10.1297

Implementing Choice Based Graphical Password Authentication in Social Networking Site

[1]*Shilpi Sharma* and [2]*J.S. Sodhi*

[1]Department of Engineering and Computer Science, ASET, Amity University, Noida (U.P), India
[2]Assistant Vice President, AKC, Data Systems, Amity University, Noida (U.P), India

Abstract: Information security is supported largely by passwords which are the principle part of the authentication process. To overcome the vulnerabilities of traditional methods, choice based graphical password schemes have been developed. This paper provides guidelines for implementing an authentication system for data security at profile login in context to social networking sites. The proposed framework works on choice based graphical authentication, which is an alternative authentication method to text based systems. Click based graphical password provides security from brute force and dictionary attacks and they are not predictive thus it's not easy to breach them. A sound signature is integrated along with it. It enhances the security as this sound signature also under goes the password verification and once the graphical password along with the sound signature is verified, the user is allowed to log into the social media profile. This paper will then compare and evaluate these approaches with text base systems in terms of usability and security. To achieve this goal a survey was conducted by distributing a questionnaire to 100 participants. The data was analyzed via SPSS. Results from our evaluations, though not conclusive but suggest promise that choice based graphical passwords can resist attacks more than text based password authentication.

Key words: Authentication · Encryption · Social Networking Sites

INTRODUCTION

Passwords are used for Confirmation, Approval and Access Control. Most of the users select passwords that are easy to predict. Users chooses unforgettable password, which means the passwords follow predictable patterns that are easier for attackers to guess. This information can be used by malicious users, fraudsters, or it can be used to make scammers seem genuine [1]. The predictability problem can be solved by restricting user to choose from predefined passwords and assigning passwords to them.

Many password systems have been developed. Study shows that, textual passwords suffer with both safety and usability troubles, as users have a propensity to pick short passwords or passwords that are easy to memorize in social networking sites, which makes the passwords insecure for attackers to crack. In social networking sites during profile log in it is easy to presume the text password for user's authentication which is vulnerable to various attack methods such as dictionary attack, brute attacks, social engineering attacks and shoulder surfing [2, 3]. Hence, the graphical password can be used as a solution [4, 5]. In an article, a security team at a company used a network password cracker and they identified about 80% of the passwords within 30 seconds. It is a well-known verity that the human brain identifies and remembers images better than text, thus using images as password is a better approach than textual passwords [6].

Considerable work has been done in this vicinity. One of the best known of these systems is Passfaces, which shows the operation of a graphical password recognition system [7]. Blonder-style passwords are based on cued recall that a user clicks on several previously chosen coordinates in a single image to log in. As implemented by Passlogix Corporation, the user needs to select several predefined regions in an image as his or her password and to log in, the user has to click on the same area.

The problem that continues in this scheme is that the number of predefined regions is small, thus the password must have about 12 clicks for adequate security which is again a tiresome task for the user. Another

Corresponding Author: Shilpi Sharma, Department of Engineering and Computer Science, ASET, Amity University, Noida (U.P), India.

drawback of this system is the need for the predefined regions to be voluntarily restricted. In effect, this would require abstract, artificial images rather than complex, real-world scenes, thus limits the user's space from choosing the images for creating a secure and easy to recognize password.

An alternative method to Passfaces scheme was Cued Click Points (CCP), where the user can click only one point or the number of points on one single image. Thus it offers cued-recall and introduces visual cues which instantly alert the valid users if they have made a mistake when entering their latest click-point and then at that point they can cancel their attempt and retry from the beginning. But his method also has more drawbacks like false accept (the incorrect click point can be accept by the system) and false reject (the click-point which is to be correct can be reject by the system). User testing and analysis showed no evidence of patterns in CCP [8], so pattern-based attacks seem ineffective.

In order to overcome the problems, a new method called Choice Based Graphical Password is proposed for user authentication at login in social networking sites. The user can click only one single image along with typing the text password that was stored in the server database in an encrypted form. Thus, we consider offering additional security over text passwords to provide better systemic usability and memorable to the users.

The structure of the present paper is as follow. In section 2 we discussed the related work in textual and graphical passwords, section 3 illustrates the paper methodology to collect the data and section 3 describes the results with discussion. Finally, section 4 presents a proposed architecture and section 5 presents a conclusion.

Related Works: Data security has been a prime concern in social networking sites such as Facebook, Linkedin, Twitter, My Space etc. Although various algorithms and tools are available to secure data, it is however being intruded or data being hacked by other legitimate users.

Following are some approaches which were proposed earlier:

Recognition Based Techniques: A graphical authentication scheme proposed by a Dhamija and Perrig was based on the concept of Hash Visualization techniques. In that system, the user was asked to select a quantitative number of images from a set of program generated images. Later, the user was prompted to identify the pre-selected images in order to get authenticated. The results reflected that 90% of all participants had successfully identified this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach. The system had to store a huge data in order to store images for each user which was the major drawback of the technique. Even the selection of images for each user from the picture database is a challenging task and needed a lot of computation time [9].

Passface: "Passface" is another technique which was developed by Real User Corporation (accessed in May,2014). Basic ideology of this technique is that the user will be asked to choose four images of human faces from a database of face images as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated only if he identifies the four faces correctly. It is based on the assumption that people can recall human faces easier than other pictures. Valentine in his User studies in 1998-1999 have shown that Passfaces are very memorable over long intervals. However the effectiveness of this method is still uncertain.

Davis, *et al*. [10], studied the graphical passwords created using the Passface technique and some obvious patterns were found among these passwords. For example, most users tend to choose faces of people from the same race. This makes the Passface password somewhat predictable.

Convex Hull of Pass Objects: The method was given by Sobrado *et al* [11] to develop a graphical password, which deals with the shoulder-surfing problem. In the first scheme, the system displays a number of pass-objects which are pre-selected by the user among many other objects.. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. To make the password hard to guess, Sobrado and Birget suggested the use of 1000 objects, which makes the display very crowded and the objects are almost indistinguishable and using fewer objects would lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user needs to move a frame until the pass object on the frame lines up with the other two pass-objects. It is also suggested to repeat this process a few more times to

minimize the likelihood of logging in by randomly clicking or rotating. The major drawbacks of these algorithms are the slow log in process.

Et-al Graphical Password: Man, *et al*. [12], proposed another graphical password system. In this system, 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 variants present in the scene as well as a code indicating the relative location of the pass-objects. The advantage of this technique is the almost impossible probability to crack this kind of password even if the whole authentication process is recorded on video because there 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. [13, 14].

Draw a Secret: Jermyn, *et al*. [15], proposed a technique, called "Draw - a - secret (DAS)", which allows the user to draw their unique password. A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. The user is authenticated if the drawing touches the same grids in the same sequence. The major drawback of this system is the hard to remember drawing sequence.

Based on the literature review, this paper summarized the impact of combined graphical authentication in social networking sites as in Table 1.

Proposed System Overview: The system proposed here is a multi-layered system to strengthen security in social networking sites. The system intends to create a graphical password using single/multiple images. Password is generated by assigning click points in each image and SQL server is used to maintain user's database and provide another security layer. Steps for creating and verifying choice based graphical password:

- Identify an image from matrix of images and choose a textual password.
- Redirect the image and the textual password generated to the SQL database after performing encryption.
- After this the user enters his textual password and click on the preselected image to verify him-self at logging in social networking site.
- The given input is verified by the SQL server that is stored in an encrypted form into database records.

Implementation

Objective of the Paper: The objectives and purpose for this paper is to analyze the existing password systems and suggest a new combined graphical password system which would enhance the security and smoothen the working in social networking sites. This not only focuses on security maintenance of the data in social networking site but also keeps in mind about the resources which are being used thus focus is on complete optimization of graphical password system.

With the new developments, the accent on building very secure system is paramount since services are not on client's computer and the server would need to know who is an authorized user. So, the proposed framework will authenticates user while logging in social networking

Table 1: Comparison of Existing Systems

Technique	Usability	Drawback
Text based Passwords	Typing alpha numeric password	Dictionary attack, brute force search, guess, spyware, shoulder surfing
Recognition based technique	Pick several pass-pictures out of many choices.	Takes longer to create than text password, creates heavy load on database to store many images.
Passface technique	Recognize and pick the pre-registered face images.	Very much predictable, creates load of decoy faces on database.
Convex hull formed by pass objects	Click within an area bounded by pre-registered picture objects	Hard to remember when large numbers of objects are involved.
Man et-al graphical password	Type in the code of pre-registered picture objects	Needs to memorize both picture objects and their codes. More difficult than text-based password
Draw a secret	Users draw something on a 2D grid	User studies showed the drawing sequence is hard to remember

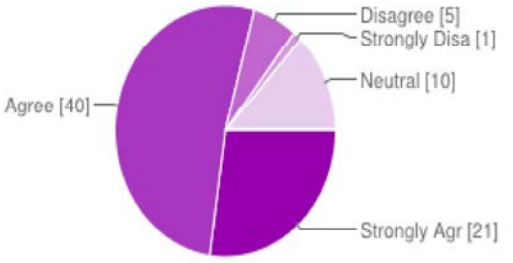

Fig 1: Pi- Chart of user's response

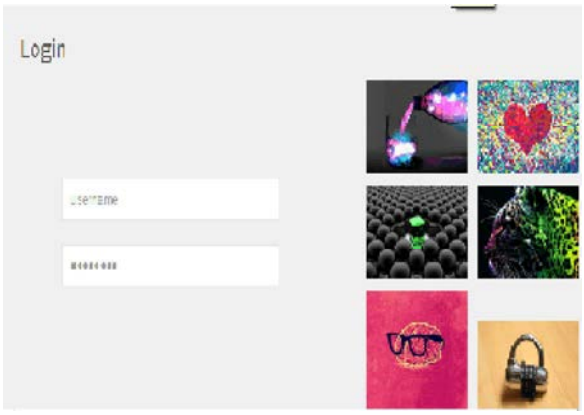

Fig 2: Choice based graphical password along with textual password

site using text-based passwords and choice based graphical image. At the time of profile creation the user will select an image of his choice from an array of images as shown in figure 2. Along with the textual password, the chosen image will be encrypted and stored on the server.

Text based passwords suffers with both security and usability problems [16]. The framework is benefited by combining graphical password with text password at login in social networking sites, might proves useful. The framework includes better password strength (space), better protection from key logging attacks, protection from phishing and man in the middle attacks. It consists of a regular text login followed by a graphical component. For logging in the social networking site, the user will choose one image from a grid of images, called TwoStep concept which is similar in concept toPassfaces [17]. Also, In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices [18, 19].

We believe that when choice based graphical password is combined with text passwords, may help to bridge the gap between security and usability. This framework also has a very good Performance in terms of speed, accuracy and ease of use.

Modules of Proposed System

User Maintenance: This module allows the registration of the users. The user's profiles are created with security accounts in the SQL Server database. Each user is associated with password. Only users having these accounts can access the application to perform any specific task, Vikram *et al*. [20].

Graphical Password Generator: The module allows the user to generate password from images. The user has to specify the required image and click on the image to generate strokes. Each stroke provides a pair of co-ordinates (x, y location) from the image. The co-ordinates in the pattern clicked and the number of strokes along with the image is redirected to the database after performing encryption. The source image can be deleted as the application does not have a direct dependency on the physical file as the image and click information has been directed to SQL database.

Verification: This module asks user to provide SQL password and then asks user to select the image from the array of images and then performs binary conversion and encryption, as the user is verified by the provided areas which helps user to recognize his authentication. It then performs encryption on click points and then compares them with the stored password.

Implementation Overview: A survey was conducted by using a questionnaire to determine the impact of attacks against choice based graphical passwords that depends on choosing from specific photo. In total, this study managed to recruit a total number of 79 participants. Majority of the participants were male with count value 47 and only 32 of the participants were female. 37 of the participants were undergraduate students; with 23 were postgraduate students and 19 were respondents from different corporate firms. They have been asked if they would like to have Graphical user authentication along with text password during login in SNS, the response is 51% user agrees to it, 27% are strongly agreed to the idea, 13% are neutral of this implementation, 6% disagreed.

Table 2: Preference of respondents

Option	User input	Percent (%)
Strongly Agree	21	27%
Agree	40	51%
Disagree	5	6%
Strongly Disagree	1	1%
Neutral	10	13%

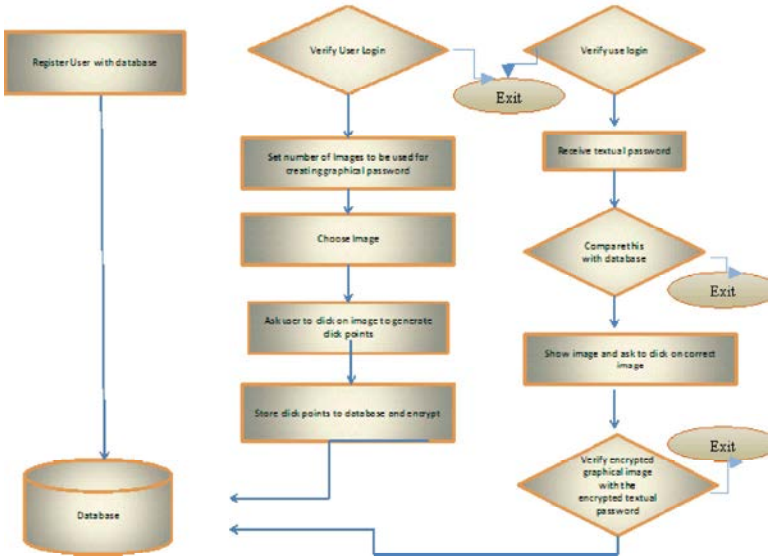

Fig 3: Flow chart of proposed Choice based graphical password.

The analysis confirmed the usability of this framework was good in terms of success rates and that respondents opinions were favorable. We additionally showed that respondents were more accurate in targeting their choice of image which significantly influenced success rates.

Architecture of Proposed System: System includes a SQL server for storing user information and graphical password, GUI is provided with the help of windows forms, which provide an interface to users to interact with the system for creating graphical password by choosing images and then providing click points. The click points undergo MD5 encryption and then stored in database.

CONCLUSION

The text based passwords are omnipresent due to ease of use, less cost, no need for special network and authentication process is known by all users, Moglen [21], William [22]. No previously developed system used this approach of logging in social networking sites. So the use of encrypted graphical images and textual passwords strengthens the security system by almost removing the chances of getting breached in social networking sites whose security system is to be enhanced. The application ensures that only a legitimate user who can provide the right SQL password can login. Graphical images for verification will be able to access his profile in social networking sites which is protected by security system. The choice based graphical password is more difficult to guess in comparison to textual and click based graphical password since there is a huge amount of photos. Thus helps legitimate users in recollecting graphical password and stops any kind of false trails of illegitimate users. In future other patterns like touch, smells may be used for recalling purpose in social networking site, as study shows that these patterns are very useful in recalling the associated objects like images or text.

REFERENCES

1. Gordon, L.A. and M.P. Loeb, 2002. the economics of information security investment", ACM Transaction on Information and System security (TISSEC), 5(4): 438-457.
2. Lashkari, A.H., A.A. Manaf and M. Masrom, 2012. "Graphical Password Security Evaluation by Fuzzy AHP," Proceedings of World Academy of Science, Engineering and Technology. World Academy of Science, Engineering and Technology.
3. Dunphy, P., 2013. "Usable, Secure and Deployable Graphical Passwords," Newcastle University PhD Thesis, pp: 1.
4. Stobert, E.A., 2011. "Memorability of assigned random graphical passwords," Carleton University (Canada), UMI Dissertations Publishing.
5. Nelson, D.L., 2004. "Use of image-based mnemonic techniques to enhance the memorability of user-generated passwords," California State University (Long Beach), Dissertations Publishing.

6. Gilhooly, K., 2005. "Biometrics: Getting Back to Business," in Computerworld, May 09
7. Brostoff, S. and M.A. Sasse, 2000. "Are Passfaces more usable than passwords: a field trial investigation," in People and Computers XIV-Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag.
8. Chiasson, S., A. Forget, R. Biddle and P.C. van Oorschot, 2009. "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," International Journal of Information Security, 8(6): 387- 398.
9. Dhamija, R. and A. Perrig, 2000. "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium.
10. Davis, D., F. Monrose and M.K. Reiter, 2004. On User Choice in Graphical Password Schemes.13th USENIX Security Symposium.
11. Sobrado, L. and J.C. Birget, 2002. "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, pp: 4.
12. Man, S., D. Hong and M. Mathews, 2003. "A shoulder-surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV.
13. Shrikala, P.R.D., M. Deshmukh and A.B. Pawar, 2013. "Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme," International Journal of Soft Computing and Engineering (IJSCE), 3(2): 2231-2307.
14. Chitrey, A., D. Singh, M. Bag and V. Singh, 2012. "A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model," International Journal of Information & Network Security (IJINS), 1(2): 45-53.
15. Jermyn, A. Mayer, F. Monrose, M.K. Reiter and A.D. Rubin, 1999. "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium.
16. Chandrashekar Singh, 2011. Lenandlar Singh, "Investigating the Combination of Text and Graphical Passwords for a more secure and usable experience", International Journal of Network Security & Its Applications (IJNSA), 3(2): 78-95.
17. Van Oorschot, P.C. and T. Wan, 2009. TwoStep: An Authentication Method Combining Text and Graphical Passwords. MCETECH 2009, pp: 233-239.
18. Kamlesh Borkar, Ashish Damke, Bhakti Sawarkar, Prashnnaki Gedam and Akash Wankhede, 2013. "Id Wisdom through Click Based Graphical Password Authentication", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-6, January 2013, pp: 210-213.
19. Khundrakpam Johnson Singh, 2013. Usham Sanjota Chanu,,"Graphical Password or Graphical User Authentication as Effective Password Provider", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 9 September 2013, pp: 2765-2769.
20. Vikram Verma, Shilpi Sharma," 2013. Authentication System with Graphical security and sound Signature", International Journal of Computer Applications (IJCA), 66, 5(March 2013), pp: 13-16
21. Moglen, E. 2013. Privacy and security the tangled web we have woven. Communications of the ACM, vol. 56, 2 (February 2013), ACM Press, New York, pp: 20-22.
22. William, C., 2013. Rethinking Passwords. Communications of the ACM, vol. 56, 2 (February 2013), pp: 40-44.