Special Issue | August 2017 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

All India Seminar on

Futuristic Trends in Telecommunication Engineering & Telecom Panorama – Fundamentals and Evolving Technology, with Particular Reference to Smart City on 5th – 6th August 2017

Organized by

The Institution of Engineers (India)
Jabalpur Local Centre

Image and Pattern Based Multi-Factor Authentication

Dileep Kori
M.Tech. Scholar
Shri Ram Institute of Science & Technology
Jabalpur (M.P.), [INDIA]
Email: dileep_kori@yahoo.com

Prateek Gupta
Associate Professor
Department of Computer Science
Shri Ram Institute of Science & Technology
Jabalpur (M.P.), [INDIA]
Email:pguptace@yahoo.com

Abstract—*Graphical passwords are a form of user authentication on which a lot of research has been undertaken over the past decade and a variety of alternative password schemes proposed. Proposed system develops image based and pattern based authentication method. It provides user to select image and grid pattern for making pattern password. It was found that brute-force attacks were largely ineffectual in terms of time required although image analysis had a profound impact on the effective password space. Password generated by this algorithm is more memorable than pass point mechanism. Proposed system is user friendly, effective, efficient, multifactor and multilayer authentication system. It keeps resistance against information leaks, brute force attack, phishing attacks, replay attack and man-in-the-middle attack.*

Keywords:—*Security, Authentication, Multifactor authentication, Graphical authentication.*

1. INTRODUCTION

Internet services such as social networks, e-banking, email, cloud services, blogs, all require some form of user authentication. Despite the availability of advanced authentication technologies such as smart cards, biometrics or USB tokens, passwords and PINs are still the most prevalent form of user authentication. In general, information sharing applications rely on variety of identifiers that combined, allow the application to authenticate and authorize access to the data. Several secure password selection approaches that take into account usability, have been proposed but the mechanisms are mostly complex and result in users developing alternative coping behaviours that lead to insecure systems. For instance, users typically use the same “easy-to-remember” password across different web applications because of the difficulties the users face in recalling the password and the wait-time typically required to receive permission to reset the password.

Studies have shown that graphical passwords are a better alternative to text-based passwords from the memorability and usability perspective [1]. Furthermore, psychologists have shown, with both recognition and recall tasks, that image are more memorable to humans than words or sentences [2]. Both these arguments make graphical passwords a good alternative to consider over text-based passwords with respect to authentication mechanisms for information sharing applications. In This paper we propose a New Graphical Password Based on Pattern drawing factors that will provide more security towards authenticating a user.

A. Overview of Graphical Password:

Graphical passwords can be classified under three categories namely, recognition, recall, and cued-recall. Recognition schemes operate by requiring the user to recognize visual data. Recall schemes require the users to reproduce something that was created earlier during registration, and finally, cued-recall schemes provide the users with some clues to aid recollection. Application examples for graphical password use as an authentication mechanism emerge in social media, online commerce, and also in the management of critical infrastructure such as smart micro-grids. In all of these applications, the underlying access control model is discretionary, and so the onus of protecting one's content from adversarial access lies with the user who is making the content available.

B. Graphical Password Authentication:

According to its working mode, graphical password authentication schemes can be classified into two types: recognition-based and recall-based graphical techniques.

Recognition Based Techniques: Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. There are many graphical password authentication schemes which designed by using recognition-based techniques. We only introduce two typical schemes. The first one is PassFaces which was developed by Real User Corporation [3]. The user will be asked to choose four or more images of human faces from a face database 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 cheat faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures.

Another recognition-based scheme is Pass-Objects which were developed by Sobrado and Birget [4]. The system will display a number of pass-objects among many other objects. Then, to authenticate, the program shows a variety of similar objects on the screen, and the user is asked to click inside the area that the selected objects make. For instance, if you chose three Pass-Objects, when those three objects are displayed on the screen, it will form a triangle. What a user will then do is click inside of this newly formed invisible triangle for authentication. It will then ask for the same action again, but with the icons on the screen in different positions.

2. RELATED WORK

A) Estimation criteria:

The estimate criterions of graphical password authentication scheme include its security, usability, reliability and availability [5].

1) Security: The security is the most important and basic request for authentication scheme. It is designed large password space, some effective method which can fight back possible attacks, some way to prevent graphical password from revealing.

2) Usability: The graphical password must be designed convenience for user to remember it.

Furthermore, because the graphical password system needs to spend more steps and time during the registration stage, the authentication process of it is more complicated than that of the text password system. To solve the problems the graphical password system must be designed easy to use for users.

3) Reliability: The major design issue for graphical password especially for the recall-based scheme is the reliability and accuracy of user input recognition. In this type of scheme, the error tolerances have to be set carefully. Because higher tolerances may lead to higher positives while lower tolerances may lead to many false negatives. Also, more error tolerant may lead to more vulnerable it is to attacks.

4) Availability: The 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 scheme in which a large number of pictures may need to be displayed for each round of verification. So it is important to solve the availability problems.

In 2015, Doiphode et al [6] proposed a scheme that combines Captcha and graphical password. For example, suppose the password is "Mango". During sign in user see the Captcha challenge. The m, a, n, g, o are at different locations and there are different alphabets too. User clicks on the locations of the m, a, n, g, o in correct sequence.

Advantage

It is prevents from the attacks of bots and guessing [5].

Disadvantage

It is non-resistant to shoulder-surfing attack.

B) Graphical Pass Points Methods:

PassPoints was first proposed by [7] utilising a series of click points on a background image to compose a password. Although it uses a similar concept to schemes proposed by Blonder (1996) among others, it allows for more choice in selection by allowing users the freedom to click on any point on the image rather than on pre-defined objects, also giving the password more entropy. This was achievable through the introduction of discretization of points using a grid which allows secure hashing of the password and allowing a tolerance amount from the click points stored meaning that users don't need to be accurate to the exact pixel coordinate when entering their password. Usability tests have found that although password retention rates were quite good using this system over periods of several weeks, users still had more difficulty learning their passwords and took longer to input them compared to control tests undertaken with alpha-numeric test users. It has often been suggested, that slower login speeds and errors with PassPoints are partially caused by users general lack of familiarity with graphical password systems in comparison to the widely ingrained use of alpha-numeric passwords and there have been indications that login and password creation speeds have improved with continued use [7].

Chiasson, Biddle and van Oorschot found in a later usability study that the choice of background image used had a profound effect on user's ability to successfully remember and input passwords over periods of time [8]. Users in their studies have indicated a preference for images with numerous distinct features, high contrasting elements, structural lines, repeating patterns, numbers and letters to provide a wealth of options in choosing clickable points they could remember. Birget, Hong and Memon [9] considered allowing users to "upload" their own background image rather than being limited to the ones provided by the system. However Chiasson et al. [10] in their 2011 paper reviewing graphical password schemes, suggested that inability to enforce a new image selection upon a user when resetting their password was an argument against it.

Another aspect of keen interest is the effect on memory interference stemming from having to remember and use several different passwords. This also has to be considered for the PassPoints scheme, since the unsafe practice of users reusing passwords across different accounts is one of the aspects of usable security which graphical passwords such as PassPoints were designed to address. It would make sense that reusing the same background image for multiple different passwords may impede a user's ability to correctly retain both passwords in memory as the same image features will appear in both and interference is more likely. A study on the issue of multiple password interference using PassPoints by Chiasson et al. [11] found that in comparison to alpha-numeric passwords, users were, in at least some of the retention trials, more capable of inputting their password correctly when they had to remember six using different background images. It was noted that the fact that PassPoints utilised background images to cue the user's memory of their password, helped in the short term and users did not cycle through their passwords since they used distinct backgrounds although after a few weeks, results stabilised and a sizable amount of both text and PassPoints users alike had forgotten their passwords (30% and 43% respectively). They stipulated that another factor besides number of passwords and the background images ability to cue memory is the frequency with which different password accounts are used.

PassPoints allows users to click on any point of an image to compose a password. These points must be stored in a cryptographically hashed form to be secure and users must be able to re-enter those same points and compare them to stored password to login. The problem arises that firstly users cannot click on the exact same point and secondly those slight variations in locations on a pixel level will result in a completely different hashed password. A potential solution would be to apply fixed grids over an image and store the grids selected by the user as the password. However the usability issue of edge cases then emerges, where users may click near the edge of a grid and get a false reject next time they try to login, selecting a neighbouring grid instead.

Solutions to the issue of approximating this input data comes in the form of discretization which maps continuous data to discrete values using one of several proposed methods, the first by Birget, Hong and Memon [10] called Robust Discretization which was proposed alongside the PassPoints scheme. It works by using 3 offset grids overlaid on the 2D image, where for each point, at least one grid is identified whose edge considered r safe. Any input points within minimum tolerance r distance from the original point are guaranteed to be accepted and any points further than max tolerance are guaranteed to be rejected. However in the worst case scenario the max tolerance would be up to 5r given a grid square size of 6r. As the grids are not centered on the click point as a user might expect this leads to inconsistencies in terms of which grid an input point will fall under and the tolerance distance will therefore vary in each direction.

3. PROPOSED METHOD

A) Proposed System:

Traditionally, multifactor authentication has been expensive to deploy, based on the cost of buying equipment and the time it took to enroll individuals into the systems. Proposed system is a secure multifactor authentication system using image and pattern based approach. User selects one image from predefined set of images and one pattern grid from predefined pattern grids. After this user has to draw five point pattern on pattern grid, which has to be converted into hash value and save at the time of registration in database. At the time of login, user should enter user name. If user name is valid then select image and pattern grid and draw five point patterns. System converts this into hash and matches it with stored hash. On success user is authenticated otherwise not. Proposed system removes drawback of traditional methods of authentication like one time password, biometric authentication, face recognition etc. They are costly means. One time password need some channel to send OTP like SMS. Biometric and face recognition requires extra device, they are also time expensive. Proposed system is secure, easy, efficient and cost effective also. System overview is presented in figure. Proposed system contains two phases: Registration and Authentication.

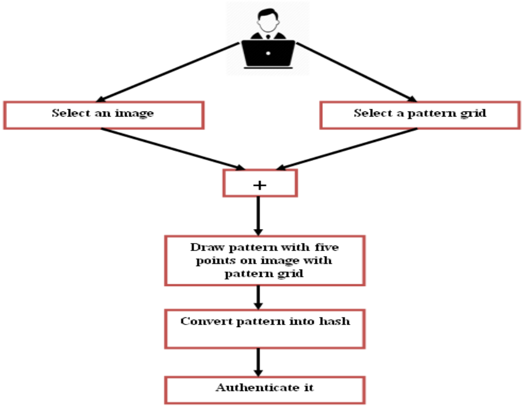
Select an image
Select a pattern grid
+
Draw pattern with five points on image with pattern grid
Convert pattern into hash
Authenticate it

Figure 1.: Proposed system.

B) Authentication Phase:

When user login in the system, system will ask for user name and checks that user exist or not. After that user should select same image, pattern grid and pattern. They are matched with stored data. If matched than user is genuine otherwise not. Steps for this process are given below:

Step-1: Enter user name.

Step-2: Check user exist or not. If exist then go for next step otherwise try again.

***Step-3*:** Select an image and a pattern grid from predefined set (which should be same that are saved at the time of registration for genuine user)

***Step-4*:** Draw five point patterns on grid.

***Step-5*:** Generate hash of pattern.

***Step-6*:** Check this hash pattern with stored pattern.

Step-7: If matched than user is genuine and open the system for further Working otherwise try again.

4. EXPERIMENTAL SETTING AND RESULTS

In registration module user enters user name, selects an image and a pattern grid from predefined set of images and pattern grid then draw pattern with five points, convert it into hash and store it. After selecting image and pattern grid, system will ask for drawing five point connected pattern. This pattern points are concatenated according to selected pattern point id and then converted into hash value. This module works for registration as well as authentication. Hash conversion module convert pattern into hash value using a secure Java PBKDF2 hashing implementation written by Hornby (2013). This PBKDF2 key derivation function is supposedly more difficult to crack, by requiring more computation on the part of the attacker to compute the hash, depending on the number of iterations used, increasing the time required for each hash computation. In pattern matching, user entered hash pattern will be matched with stored hash pattern; if they are same then user is authorized otherwise not.

A) Predefined Pattern Grid:

Proposed system uses following predefined pattern grid.

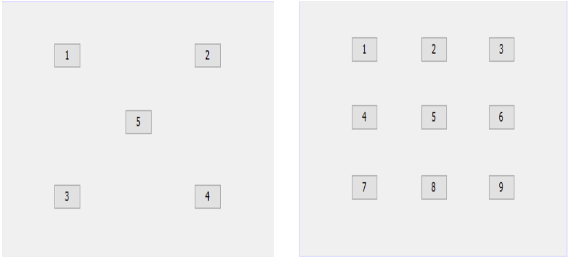

Figure 5 (a), (b): Predefined pattern grid.

Snapshot below is user interface for registration. Here user should enter user name and then select one image and one grid pattern, after that click on next button for making five point patterns.

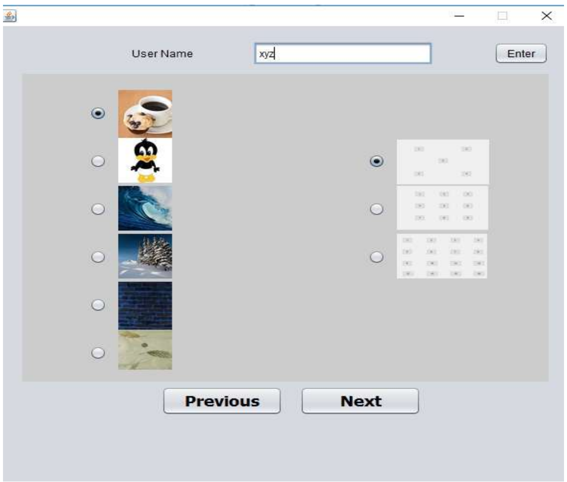

Figure 6. Registration Module.

Snapshot below is user interface for registration. Here user should enter user name and then select one image and one grid pattern, after that click on next button for making five point patterns.

B) Performance evaluation:

The proposed model for authentication solves following issues for authentication using multifactor approach. It keeps resistance against the following security hazards and susceptibility:

1. Probing, information leaks
2. Shoulder Surfing
3. Phishing attacks
4. Token theft
5. Replay Attack
6. Eavesdropping
7. Man-in-the-middle attack

C) Evaluation on the basis of Total Authentication Time:

Table 1. Sample 1

Algorithm	Authentication Time (s)
Existing Method	6.42
Proposed	4.15

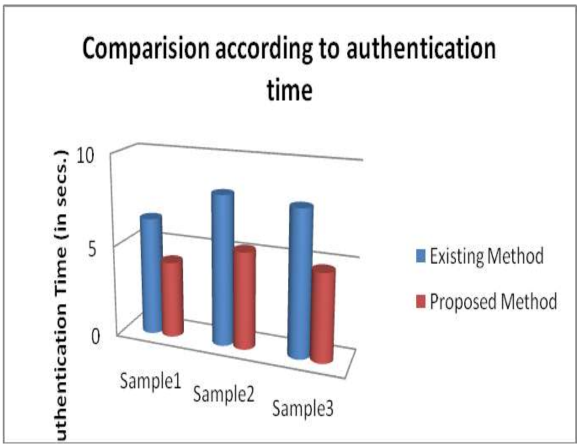

Figure 7. Comparison Chart.

Above chart will show that in every sample proposed system is time efficient then existing system. These are some aspects which, while not absolutely required for the functioning of this prototype, are still important for a viable, usable and secure authentication system implementation.

5. CONCLUSION AND FETURE WORK

Proposed work is evaluated with existing pass point method and found improved security. In terms of security I have not found the passwords to be any more prone to guessing attacks than alpha-numeric passwords. It is user friendly, efficient and most objectives have been met to a certain degree. Proposed method of authentication can be used for cloud computing, smart phone applications, touch screen device, PDA and many more fields.

An authentication implementation using two-factor authentication using a mobile device for entering the graphical password could also be a viable system worth further consideration. For mobile use, the smaller screen size has to be taken into consideration, meaning smaller images and resolutions, adjusted tolerance values and perhaps a zoom in function to accommodate the touch-screen input. It may also be used in integration with face recognition.

REFERENCES:

[1] E. Hayashi and N. Christin, “Use your illusion: Secure authentication usable anywhere,” in In Proceedings of the

4th Symposium on Usable Privacy and Security, (Pittsburgh, PA, USA, July 23-25). ACM Press, 2008, pp. 35 –45.

[2] R. Biddle, S. Chiasson, and P. Van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surv, vol. 44, no. 4, pp. 19:1–19:41, Sep. 2012.

[3] RealUser [EB/OL]. [2007-11-1]. www.realuser.com.

[4] L.Sobrado and J.-C.Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[5] J.C. Birget, D. Hong, and N.Memon, "Graphical Passwords Based on Robust Discretization," IEEE Transactions on Information Forensics and Security 1(3), 2006, pp.395-399.

[6] Elham Darbanian, Gh. Dastghaiby - fard," A Graphical Password against Spyware and Shoulder-surfing Attacks", IEEE 2015.

[7] Wiedenbeck, S., Waters, J., Birget, J. C., Broditskiy, A. and Memon, N. Authentication Using Graphical Passwords: Basic 29March 2013.

[8] Chiasson, S., Biddle, R. and van Oorschot, P. C. "Graphical Passwords: Learning from the First Generation", (2009)

[9] Birget, J. C., Hong, D. and Memon, N. "Graphical Passwords Based on Robust Discretization" (Accessed: 18 October 2013).

[10] Chiasson, S., Biddle, R. and van Oorschot, P. C., "Graphical Passwords: Learning from the First Twelve Years", 2011.

[11] Chiasson, S., Forget, A., Stobert, E., Van Oorschot, P. C. and Biddle, R. "Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords", Carleton University-(2009).