IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. IX (Mar-Apr. 2014), PP 124-128
www.iosrjournals.org

Image Based Authentication for Folder Security using Persuasive Cued Click-Points and SHA

[1]Suraj Hande, [2]Nitin Dighade , [3]Ruchal Bhusari, [4]Mrunali Shende,
[5]Prof. Heena Agrawal
[1,2,3,4]Student, Dep. of Computer Technology, Rajiv Gandhi College of Engineering & Research, RTMNU Nagpur, Maharashtra, India
[5]Lecturer, Dep. of Computer Technology, Rajiv Gandhi College of Engineering & Research, RTMNU Nagpur, Maharashtra, India

Abstract: *In this paper Image Based Authentication application is applied on folder's (folders that are confidential to user) ,since the studies till date have shown that textual passwords are more prone that they are well hacked by hackers through easily available software's or programming different code to hack the password.*
The textual passwords use languages that can be identified using the grammar that they use, therefore our project focuses on Graphical passwords , because as such it has been observed that human brains is better at re-collecting and recognizing images than text, the images are well captured and stored rather than text. There have been phases in creating a strong graphical password scheme from 1999, with the promise that the graphical passwords would provide improved password memorability and usability.
The technique that we use here is PCCP (PERSUASIVE CUED CLICK POINTS), this is a combination of recall and recognition based techniques with the implementation of SHA1 (Secure Hash Algorithm). Here PCCP is used for user to have better strong passwords by expanding password space and SHA1 is used to ensure security to folder.
Keyword: *Authentication, Graphical Password, Hotspot, Passpoints, Secure Hash Algorithm,*

I. Introduction

Current secure systems grieve because they ignore the importance of human factors in security. An ideal security system reflects security**,** reliability, usability, and human factor. The knowledge based authentication system includes the text passwords and graphical passwords. Typically text passwords are string of letters and numbers, i.e. they are alphanumeric. Although text passwords should be both memorable [7] and secure, in practice, most passwords are either memorable but easy-to-guess or secure but difficult-to-remember.

A password authentication system should encourage strong passwords while maintaining memorability. In an attempt to create more memorable passwords, graphical password system has been developed. In these systems authentication is established on clicking on images rather than typing alphanumeric strings. Graphical passwords techniques will be categories into Recognition Based Techniques and Recall Based Techniques, further this Recall Based Techniques can be categories into pure recall based techniques and cued recall based techniques. In such systems user identify and target previously selected location within one or more images. The images act as memory hints to aid recall.

Examples include Pass Points and Cued Click Points [4] Hotspots[2] and Pattern Based attacks[6] is effective in Pass Points, while Hotspots attack is effective in cued recall based techniques. Hotspots are areas of the images that have higher likelihood of being selected by user. To overcome all these existing defects the PCCP technique came into existence. Result show that PCCP is effective at reducing hotspots and avoiding patterns[3] formed by click-points within a password, while still maintaining usability and security issues. In this project I have apply this technique for providing security to the folder, preventing unauthorized access of the user. The system also prevents damaging of the folder from the viruses and malwares.

II. Literature Review

Phases of Graphical Password Techniques

The Graphical passwords techniques[1] is divided into two categories:

2.1 Recognition Based Graphical Technique.

2.2 Recall Based Graphical Technique.

2.1 Recognition Based Graphical Technique

Graphical authentication scheme was proposed by Dhamija and Perrig based on the Hash Visualization technique. In their system, the user is requested to choice a certain number of images from a set of random pictures generated by a program. Various types of images, most particularly: faces, random art, everyday objects, and icons are used. Later, the user will be required to identify the preselected images in order to be authenticated. Humans have exceptional ability to recognize images previously seen, even those viewed very briefly. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The normal log-in time, however, is extensive than the traditional approach. A faintness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the procedure of choosing a set of pictures from the picture database can be tedious and time consuming for the user. Recognition-based systems, also known as cognometric systems or search metric systems. The scheme increases usability as it is easy to remember images but prone to replay attack and mouse tracking because of the use of a fixed image as a password, hence it's security issues arises.

2.2 Recall Based Graphical Technique

2.2.1 Pure Recall Based Technique

This concept commencing of user producing of passwords without system being providing of hints to produce passwords, the examples of pure recall technique are Draw-A-Secret technique, Grid selection, and Passdoodle.

In this section we discuss two types of picture password techniques: reproducing a drawing and repeating a selection Jermyn, et al. proposed a technique, called "Draw - a - secret (DAS)", which allows the user to draw their matchless password. A user is asked to draw a simple picture on a 2D grid using a stylus or mouse. A drawing can consist of one nonstop pen stroke or preferably several strokes separated by "pen-ups" that restart the next stroke in a different cell. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is requested to re-draw the image. If the drawing touches the same grids in the same sequence, then the user is authenticated. In this type of system the brute-force attack is possible and the impact of password length and stroke-count as a complexity property of the DAS scheme. Recall-based graphical password systems are occasionally referred to as draw metric systems because users recall and reproduce a secret drawing.

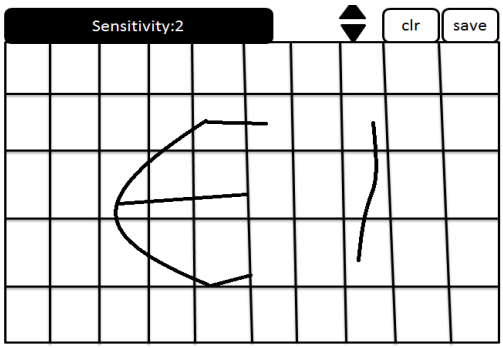

Fig.1 Draw-A-Secret

The procedure starts with drawing of objects or text that consist of pen strokes which is then differentiated with continuous pen stroke or several strokes that are separated by pen ups .Then at the time of log in these sequence of coordinates of the grid cells yields an encoded DAS password.

2.2.2 Cued Recall-based Technique

This technique initiates the system to provide a clue to the user that produces passwords, the system generates active areas where the user selects pixel points to choose the same region on the image following the same sequence to login into the system, this technique has two implementations, PassPoints and CCP but they result with pattern attacks and hotspots[2]

PassPoints

Based on Blonder's original idea, Pass Points (PP) is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel-based image. To log in, a user must click inside some system-defined tolerance region for each click-point. The image acts as a cue to help users recall their password click-points. In this technique Brute force attack, hotspot attack and pattern-based attacks is possible.

This technique uses selection of an image and sequencing of pixel in an orderely ,during login the user would remember the sequence of pixel that had entered during the time of creation of password .This makes easier for the attackers to predict the pixels.

Fig.2 On passpoint,a password consists of 5 ordered points on the image (the numbered labels do not appear in practice)

CCP (Cued-Click Points)

CCP was developed as an alternative click based graphical password scheme where users select one click-point on each of 5 images presented in sequence, one at a time; this provides one-to-one cueing. Every image next the first is a deterministic function of the current image, the synchronizes of the user-entered click-point, and a user identifier. Users receive immediate feedback if they enter an incorrect click-point during login, seeing an image that they do not identify. At this point they can restart password entry to correct the error. This implicit feedback is not helpful to an attacker not knowing the expected image sequence. In this technique more possibility of hotspot attacks. To overcome this problem a new technique of Persuasive Technology is use .This initiates with selecting of pixels from a sequence of images presented to the user. Further from the first image the selected pixel value[9] generates another image of the same sequence This ensures user's usability but vulnerable to brute force attack

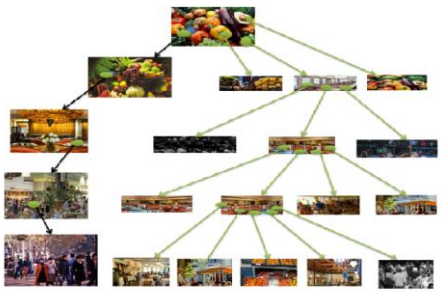

Fig.3 Selection of Click Points in CCP

III. Approach

Persuasive cued click points (PCCP)

As we have seen above in literature survey , in CCP there exist the guessing attack, capture attack, and hotspot problems which reduces the security of graphical password schemes and to overcome all above this paper proposed the design, implementation, and evaluation of knowledge-based authentication mechanism i.e., PCCP with folder Cryptography. The persuasive technology was first proposed by Fogg to make better authentication method. Visual attention research shows that different people are attracted to the same predictable areas on an image i.e hotspots , if users select their spot own click-based graphical passwords without guidance, hotspots [2] remains as an issue. PCCP system influence users to select any random click-points while maintaining usability. Here the prediction of password is difficult for the attacker as password is generated from random images. The goal was to encourage users to behave more securely by using their own choice.

Persuasive cued click points in which a password consists of five click-points, one on each of five images. While creating password , or registration most of the image is dimmed except for a small view port area that is randomly positioned on the image as shown in figure[3]. Users have to select a click-point within the view port, and they cannot be able to click anywhere outside the viewport i.e. outside the view port clicking action does not work. Viewport is nothing but a framed area. Within that random view port range there would be several tolerance squares per image or we can say tolerance area, tolerance area is nothing but the collection of all points closed to the clicked password point. If they are unable or unwilling to select a point in the current

viewport, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots[2]. A user who is determined to reach a certain click-point may still shuffle until the viewport moves to the specific location.

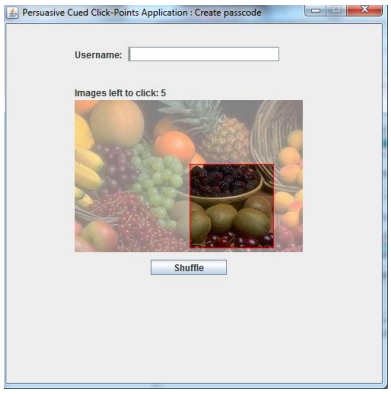

Fig.4. Password creation User interface

3.1 Secure Hash Algorithm

In our paper presents providing security to the folder so that unauthorized user unable to open the file without permission the SHA used by the software for folder security that is used for folder security in java. , we can design a software model which provides image based authentication as well as encrypting folder using Secured Hash Algorithm.

It is a hashing algorithm designed by the United States National Security Agency and published by NIST. SHA1 is improvement in original SHA0 ,was first published in 1995. SHA1 is the most widely used SHA hash function, although it is potentially more secure SHA2 family of hashing functions. Presently ,It is mostly used in a variety of applications, including TLS, SSL, SSH and PGP. SHA1 outputs a 160bit digest of any sized file or input. In construction it is similar to the previous MD4 and MD5 hash functions, in fact distributing some of the initial hash values. It works on a 512 bit block size and has a full message size of 21 bits.

IV. Methodology

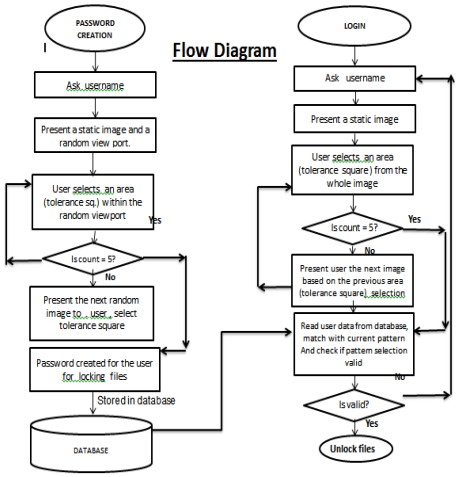

Fig4. Flow Diagram for Registration and Login Process

This system provides high security uses concept of PCCP .

Steps for password creation :

1) For creation of passwords user is presented with a single image with highlighted a random view port (an area in the image) say of 4cm x 4cm for the user.

2) In random view port there will be a tolerance squares per image (say, 1 x 1 cm).Tolerance square image will be constant for the image.

3) User selects a tolerance square within view port and presented with next image.

4) In the next new image user performs above step 1 to 3 , until the user is presented with 5 such images.

5) When user completed with the selection, that information saved in a database.

While login user must select correct sequence of click points. This is difficult for attackers because the sequence cannot predictable. If user select wrong click point ,then it will be known after completion their selection of all click points.

Login for username process consist of following steps:

1. while login , user will be presented with the same initial image but here NO view port and obviously with no shuffle button provided only all the tolerance squares will be effective.
2. Now the user selects his choice in the first initial image and according to previous click next related image will present to the user for next selection.
3. When the user completed with 5 sequential images, and the selections matches with user's stored information in database then things would unlock.

V. Application

- This method of authentication can be use for windows security purpose ,drive cryptography , online section etc,
- In online services, user have to register and maintain accounts of each website saparately before accessing its resources, user have to remember the passwords of this no of accounts .
- To remember the passwords user set either simple password or alphanumeric, sometimes same for all accounts.
- This authentication method applicable in network related application ,also use where high security required such as banking sector etc.
- This paper presents our application of method of authentication applicable for folder security.

VI. Conclusion

User authentication is a fundamental component in most computer security contexts. In our paper we proposed a simple graphical password authentication system which provides the more secure authentication than the text password scheme. We described the system operation with implementation of PCCP and trying to implement SHA Algorithm for folder security. PCCP tool such as PCCP's viewport (used during password creation) cannot be exploited during an attack. The approaches discussed in this paper present a middle ground between insecure but memorable user-chosen passwords and secure system generated random passwords that are difficult to remember. Better user interface design can influence users to select stronger passwords. The PCCP technique and Secure Hash Algorithm provides an environment in which the folder will be in safe condition. While encrypting the folder, it will be converted into zip file and then encrypted, which will not allow entering any viruses and making damage to the files present in the folder. It will be one of the safe mechanisms for folder security.

VII. Future Enhancement

- We can provide security to files.
- We can provide security for Internet Banking.
- We can secure our network in cloud computing.
- We can secure our ATM account.

References

[1]. P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe. Purely automated attacks on passpoints-style graphical password. IEEEE Trans. Info. Forensics and security, vol. 5, no. 3, pp. 393-405, 2011

[2]. K. Golofit. Click password under investigation. 12th European Symposium On Research In Computer Security, LNCS 4734, Sept 2007.

[3]. S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. User interface design affects security: Patterns in click-based graphical passwords. International Journal of Information Security, Springer, 8(6):387-398, 2009

[4]. S.Chiasson, A. Forget, and R. Biddle. Graphical password authentication using cued click points. Symposium On Research in Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359-374.

[5]. A. Dirik, N. Menon, and J. Bireget. Modeling user choice in the passpoints graphical password scheme,. In 3rd ACM Symposium on Usable Privacy and Security (SOUPS), July 2007.

[6]. Alankrita Ladage, Swapnil Gaikwad, Prof. A. B. Chougule. Graphical Based Password Authentication. International Journal of Engineering and Technology, vol. 2, Issue 4, April 2013.

[7]. Nelson, D. L., Reed, U.S., and Walling, J. R. Pictorial Superiority Effects. Journal of Experimental Psychology. Human Learing and Memory 2(5), 523-528, 1976.

[8]. Karthhik. K, Keerthana. R, Porkodi.A, Udhayakumar. S, Kesavan. S, Mr. Balamurugan. P.Defenses against Large Scale Online Password Guessing by Using Persuasive Cued Click Points. International Jounral of Computer Science and Mobile Computing.