Login Authentication System using Captcha as Graphical Passwords Techniques

Prof.Sharmila Chopade ,Assistant Professor, Department of Computer Engineering, DYPIET,Ambi, Pune, Maharastra, India1.
Prof.Rupali Adhau Assistant Professor, Department of Computer Engineering, DYPIET,Ambi, Pune, Maharastra, India2.
Prof.Chhaya Gochade Assistant Professor, Department of Information Technology, DYPIET,Ambi, Pune, Maharastra, India3

Abstract:- Now a day, vulnerability is a major issue in information and computer security. The use of internet is increasing day by day. The user selects a password for security purpose, that password is text or graphical passwords. Mostly user uses text password because that are easy to remember, but the main drawback of using a text based password and graphical password is vulnerable to many attacks. So another technique is developed which is captcha. To overcome the limitations of the captcha new technique is developed which is CaRP (Captcha as Graphical Passwords).CaRP is a combination of captcha and graphical password. It is clicking an event which is performed at various points on image in the sequence to get a new password. In this system, Animal gird is used for user authentication, which is a type of CaRP techniques and Login history is used for transaction system for enhancing the more security level primitives.

Keywords: Graphical password, password, CaRP, Captcha, security primitive, Animal grid, Login history.

I. INTRODUCTION

Authentication is the process to allow users to confirm their identity for any web application. Human factors are considered to be the weakest part of a computer security system. The three major
areas where human computer interaction is important are: authentication, security operations, and developing secure systems. Here we focus on the authentication problem. A password is a secret authentication data which are used to control access to a resource. The password is kept secret from those who are not allowed access, and those who wish to gain access to the resource are tested on whether or not they know the password and are granted or denied access accordingly.

Traditional textual password or PIN, however, relies on the keyboard as the input device. Many researchers there by look at an alternative approach graphical password. The password input is convenient as well as it is more user friendly in terms of memorability and recall ability. The main motivation for graphical passwords is the hypothesis that people are better at remembering images than artificial words; in addition, graphical password utilizes an easier and more human friendly memorization strategy recognition based memory, instead of a recall based memory for textual password.

The main motivation for graphical passwords is the hypothesis that people are better at remembering images than artificial words. Visual objects seem to offer a much larger set of usable passwords. For example, user can recognize the people, which he knows from thousands of faces; this fact was used to implement an authentication system. As another example, a user could choose a sequence of points in an image as a password; this leads to a vast number of possibilities, if the image is large and complex, and if it has good resolution.

To overcome the shortcomings of text based passwords, animal grid to login history image as a graphical password system 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 resistant to attacks such as dictionary attacks. Many graphical password schemes are already introduced. 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. The paper covers the graphical password used in authentication system; there are chances of attacks on graphical password also so to overcome this new technique introduced login history image; after the user select right image in question which are provided to him/her then only user can enter into the system..In this system only choosing the correct image of last login time and last logout time permission to enter into main system of transaction.

Paper is organized as follows. Section II describes types of graphical password techniques and captcha. Section III represents a system overview which is included system architecture and mathematical model. Section IV presents experimental results showing results of images tested. Finally, Section V presents conclusive.

II. RELATED WORK

A.Graphical Password Techniques

Graphical password techniques are developed to overcome the limitations of text-based passwords. Graphical passwords consist of recognizing the images or sometimes to recognize the image and click the particular points or area on the image rather than typing the characters like text-based password. In this way, the problems that arise from the text-based passwords are reduced. Graphical password techniques are categorized as follows: i) Recognition Basedscheme ii) Recall Based scheme iii) Cued Recall Based scheme.

A recognition-based scheme has to select the certain number of images from a set of random images in an order as a password, and for authenticating the user has to identify (recognize) those images in a same order. There are three schemes under this system: i) Method 1:

Dhamija and Perrig proposed a graphical authentication technique depends onto the hash visualization method. In their system, the user is asked to select a certain number of images from a set of random images generated by a program. The user will be required to identify the preselected images in order to be authenticated. ii) Method 2: Sobrado and Birget developed a graphical password scheme work with the surfing shoulder problem. In the first technique, the system will show a number of passes-objects. A user needs to recognize pass- objects and click inside the outside hull formed by all the pass-objects for authentication. iii) Method 3: "Passface" Real User Corporation developed these techniques. The idea is as follows: The user will be asked to choose four images of human facing as their future password security.In authentication stage, the user sees a grid of nine faces, consisting of one face previous chosen by the user & eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. A recall-based scheme requires a user to reproduce something that he created or selected earlier during the registration stage. Three techniques are: i) Method 1: "Draw-A- Secret (DAS) Scheme" Here the user will draw a simple picture on 2D grid. The coordinates of a grid are occupied by the picture are stored in the order of the drawing. During authentication, the user will be told to re-draw the picture. If the drawing touches the same sequence, then the user is authenticated. ii) Method 2: "Signature Scheme" Here authentication is conducted by having the user drawing their signature using the mouse. iii) Method 3: "Pass-point Scheme" Here the user will click on any place on an image to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerances in the correct sequence [3].

In a Cued-recall based scheme Pass Points [3] is a click based cued recall scheme where a user requires clicking a sequence of points anywhere on an image to create a password. At the time of authentication user require to re-clicking the same sequence. Cued Click Points (CCP) [5] is similar to PassPoints but uses one image per click, with the next image selected by a deterministic function. Persuasive Cued Click Points (PCCP) extend CCP where user has to select a point inside a randomly positioned viewport.

Graphical password has some limitations: i) Password registration and log-in process take too long. ii) Require more storage space than text- based passwords.

B.Captcha

Completely Automated Public Turing Test to tell Computers and Human Apart [1] (Captcha) finds the difference in humans and bots in solving the hard AI problems. It is a test to check user is Human and not a computer device. Captcha has two types: Text Captcha which is recognition of non-character objects and Image Recognition Captcha relies on recognition of images. i) Text Captcha: PayPal and Microsoft Captcha are both relied on background noise & random character strings to resist to automated attacks. The Captcha used by Google, Yahoo! All share similar properties, such as a lack of background noise of distortion for a character or word images and extreme crowding for an adjacent character. Random Captcha images are captured humanly reliably by site in the form of pixel, marginal probabilities and site by site covariance. EZ-Gimpy uses word images which employ character distortion and clutter. Personal print uses a low quality picture by degrading parameters to thicken, crowd, fragment and add noise to character images. ii) Image Recognition Captcha: Captcha consist of a combination of images [6]. The user has to recognize the images given to him to solving the given puzzle problem. As shown in Figure.2 user has to select the cat images as the password characters.

D.Captcha as Graphical Password (CaRP): An Overview CaRP has a new image is generated for every login attempt even for the same user. Alphabet which is used in CaRP of visual objects (E.g. Alphanumerical characters, similar animals, etc.) to generate a CaRP image, which is also a Captcha challenge. A Recognition-based CaRP technique used password is in a series of visual objects alphabet. Per view for the traditional recognition based on graphical password security, recognition based CaRP seems to have access to an infinite number of different visual objects. We present two recognitions based CaRP techniques and a variation next. A recognition-recall CaRP, Password is a sequence of some invariant points of objects. An invariant point of an object is the point that has a fixed relative position in different incarnations of the object and it can be uniquely identified by users or humans no matter how the object appears in CaRP images.

III. SYSTEM OVERVIEW

Problem Statement: To improve the CaRP System with valid authentication and enhance the Security by using images of different level of difficulty based on CaRP Technique with an animal grid as
graphical password and generate the Login History image for the transaction.

• System Architecture:

Figure 1: Architecture Diagram

As shown in the below fig.3 the system will work as follows:

• Registration Process:

First user starts the registration process, where the user fills up the information and selects at least 6 images from animal grid. The animal grid image is generated by the system from the system's database. Then the selected graphical password by the user is saved in database.

• Login Process

During the login process the first step is user entered the username and selects the image which he has selected during the registration process. Then the user selects the images from animal grid. If the selected sequence of images is a correct sequence, then only user can log into the system. Otherwise login will fail.

• Transaction Process

After the successful login user will actually enter into the system where users can perform the transaction. For that transaction user will enter details when he submits his transaction at that time 6 login history will be displayed. When the user selects the correct imagethenonly transaction is successful otherwise not. The login history image will be sent to user's mail after logout.

• Mathematical model:

Let System is S= {U, R, L, A, LO}

Where

U= Set of users R= Registration L= Login A= Animal gird LO= Login history

1) U = {u1, u2, u3, ...} Where u1 is user of system 2) R= {UN, ADD, E-ID, C}

UN= Name of users {n1, n2, n3, ...}

ADD = Address of users {ad1,ad2,ad3, ...}
E-ID = Email Address of users {ed1,ed2,ed3, ...}
C= Animal grid clicks at registration {c1,c2,c3, ..}
Where c1 is 12 numbers of animals
c1= {a1, a2, a3, ... , a12} 3) L= {UN, P, A}

UN= User name P= Password A= animal grid 4) A= {G, I, Ra}

G= It is grid and size of grid is 6×6
I is a set of animals I= {an1, an2, an3,....., an36} Ra=Random generation algorithm
5) LO={H, e, LI}
H is Login history H= {h1, h2, h3, ...}
h1= {time, date, day} e = e is a function by which we send email login history image LI= {L1, L2, L3,....} If user select correct image of login history then give him access to login successfully.

• Experimental results

We have tested our results in a suitable testing environment, where we have tested the performance of the system during the following three scenarios:
• graphical passwords
• Animal grid
• Login history
The following Figures. Shows the performance of the system during the time. The Figure shows the total time taken by the system, how enhanced the authentication of users.Figure shows that as early when only use the password for security purpose, then very less authentication is done. After that when system enhancing then security or an authentication is very high for the system.
Our system uses the animal grid as well as the login history image of last login time and logout time, which is more secure from other system which have already used like pass-point, click-text, password.
Figure. 2
The following Figure shows the performance of the system as well as how much people say that system is more secure than previous systems in the form of a percentage. Animal grid to login history image provides high security, 50% confirm that system enhancing the security as compared to the other system. when use the only animal grid as graphical password security authentication 30% people says that system is secure. And the little bit response for password and click text techniques. Enhancing the
system with time and adding technology with respect to their hardness.
Figure 3

IV. CONCLUSION

This paper presents various techniques such as textual password, graphical password, animal grid with login history image. Carp is a combination of both a CAPTCHA and a graphical password scheme. In this paper, we use the animal grid as well as login history image.Prevent the system from unauthorized user. Secure online transaction from various frauds. Enhancing the security in online shopping,, online room booking or an online air ticket booking.The usability of the system can be further improved by using images of different layers of difficulty based on the login history image of the system.

V. ACKNOWLEDGEMENT

The authors would like to thank the publishers, researchers for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure support. Finally, we would like to extend heartfelt gratitude to friends, family members.

VI. REFERENCES

• *Bin B. Zhu, Jeff Yan, GuanboBao, Maowei Yang, and NingXu, " Captcha as Graphical Passwords—A New Security Primitive Based on*
• Hard AI Problems" , IEEE Transactions On Information Forensics And Security, Vol. 9, No. 6, June 2014.
• R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys, vol. 44,no.4, 2012
• S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical passwordsystem," Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.
• L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in Proc. Eurocrypt, 2003,
• S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, 2007,
• P. C. van Oorschot and J. Thorpe, "On predictive models and user drawn graphical passwords," ACM Trans. Inf. Syst. Security, vol. 10, no. 4, pp. 1–33, 2008..
• H. Gao, X. Liu, S.Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in Proc. Symp. Usable Privacy Security, 2009, pp. 760– 767.
• M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," IEEE Trans. Dependable Secure Comput., vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.
• L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using CAPTCHA in graphical password scheme," in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010, pp. 1–9.
• S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.- R. Sadeghi, and R. Schmitz, "Breaking e-banking CAPTCHAs," in Proc. ACSAC, 2010, pp. 1–10.