ISSN:0975-9646

Captcha as a Graphical Password with Multilayered Enhanced Security by Clique Point Technique

Monica Auti[1], Prof. Sachin Patil[2]

[1,2]*Computer Department, Pune University*

G. H. Raisoni College of Engineering And Management, Chas, Ahmednagar.414001, India

***Abstract*— In this paper we present a security primitive which is a novel family of graphical password systems based on hard AI problem which is called as Captcha as a graphical passwords . It is the combination of a Captcha and a graphical password. It offers a number of security problems such as relay attacks online guessing attacks and many more. CaRP also prevents shoulder surfing attack if it is combined with dual view technology . This new security primitive offers an approach to present a well known image hotspot problem in popular graphical password systems , that often leads to weak password choices leading to leakage of password CaRP offers reasonable security which appears to fit well with some of the practical applications for improving security online.**

***Keywords*— Graphical password, Dual view technology, Shoulder surfing attack.**

I. INTRODUCTION

CAPTCHA :- Completely Automated Public Turing test to make Computers and Humans Apart. CAPTCHA is a technology which assures that only those people can pass the test and not the system computer generated (bots). The development of CAPTCHA system is to provide creative and validation tests that can be easily solved by humans and difficult for robot. There are four types of methods in CAPTCHA which is the text based CAPTCHA, image based CAPTCHA, audio based CAPTCHA, video based CAPTCHA. CAPTCHA system based on puzzle is developed by using a technique based on an image CAPTCHA .This type of CAPTCHA had developed by using HTML, JavaScript, Cascading Style Sheets . The CAPTCHA system is developed using a sequence of phases of development using evolutionary prototyping model based on SDLC.

A fundamental task in providing security is to create security primitives based on hard mathematical problems that are Computationally not tractable by the user. Captcha based on image is a method that is considered to be more easily recognized by the user as compared to Captcha based on Text [4]. User involvement is very important in designing Captcha to assure the safety of the robot (bots) attack. The concept is easy to implement and understand and difficult to be solved by the bots system.The development in applications including image-based Captcha provides more information than text-based Captcha .Generation of Captcha provides a novel approach, which provides effective and efficient algorithm providing sufficient information about the text tests for easy human recognition which is provided in the marginal probabilities and the site-to nearby- site covariance's and these quantities can be embedded into KNW probabilities, which is designed for the effective simulation process. The Captcha are the partial random realizations of the random CAPTCHA word: which start with initial random and uses Gibbs resampling to re-simulate portions of the field again and again using the KNW conditional probabilities until the word becomes readable by the human and easily understood as becoming user friendly in nature.

A graphical password is used in an authentication system that process by having the user who selects click points from the images, in a sequential order, which is represented in a graphical user interface to the user. The graphical-password approach which is also called as graphical user authentication

in which authentication is provided before login in the registration process . A graphical password is easy to be recognized by the human than the bots than a text-based password for most people. Suppose minimum of 7 character password is necessary to gain entry into a particular computer network. Instead of xtuyew65, a user might select images of the things ,the Meghalaya state, a black horse with its long bushy tails and blue sky flying birds and a scenery containing mountains and the birds flying , fish in the lake giving a visual effect and so on.

Captcha a graphical password is a click-based graphical passwords [3] where a collection of clicks in a sequential manner on an image is used to derive a password. Besides other click-based graphical passwords, images used in CaRP is a Captcha which is a challenge and it is not easily recognized by the user during login in registration process , and a new CaRP image is generated for every login attempt.The notion of CaRP is simple. CaRP can havemultiple instantiations [5].This scheme relies on multiple object classification which can be transformed to a multiple CaRP scheme . CaRPs can be built on both text Captcha and image-recognition based Captcha. A text CaRP in where a sequence of characters is used as a password like text password, but it can be done by clicking the right sequence of characters on CaRP images which is stored in the database. CaRP requires solving a Captcha challenge in every login trials. This impact on relevance can be removed by adapting the CaRP images difficulty is based on the login history of the different users account and

the machines used to log in the system which is present at different locations.

Applications of CaRP include

i. Nowadays captcha and a graphical password together can be applied on touchscreen mobiles because typing passwords is hectic, especially for secure Internet applications such as e-banks for login sessions.

ii. In the email services also this technology is used to reduce the spam emails from the inbox[6].Email service provider that deploys CaRP, a spam bot (robot) cannot login into an email account even if bot knows the password but here the involvement of user (human) is mandatory.

CaRP is a click-based graphical passwords, wherein a sequence of clicks on an image is used to derive a password in the form of pattern. Besides other click-based graphicalpasswords, images used as a password in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt. CaRP can have multiple instances. Any Captcha scheme which relies on multiple object classification can be converted to a CaRP scheme which becomes easy for original set to provide a better security.

Design Goals

1. Offers reasonable security and usability and appears to suits well with some of the practical applications which provides better security to the online applications.
2. Defence against online dictionary attacks which helps in providing the efficiency of the system.
3. CaRP offers protection against relay attacks on increasing threat to bypass captcha applications.
4. It can be used to fight against relay attacks.

II. RELATED WORK

A. *Captcha*

Captcha is capable to distinguish between humans and robots in solving certain hard AI problems which is mathematically feasible which can be solved by the user and not the bots. There are two types of visual Captcha which is recognized by human instead of bots: Captcha based on text and Captcha based on Image-Recognition.The former relies on text recognition while the latter relies on recognition of non-character object. Text Captcha relies on the difficulty of character segmentation, which is difficult to solve (expensive) and combinationally hard.

B. *Captcha in Authentication*

Captcha and password together is used in a user authentication protocol, which is called Captcha-based Password Authentication protocol, which encounter online based dictionary attacks. The CbPA-protocol is used for solving a Captcha puzzle after putting a valid pair of user ID and password until a valid browser cookie is received to the system. For a wrong pair of user ID and password, the user has a certain guessing to solve a Captcha challenge before being access is denied .

C. *A cued based recall scheme*

An external cue is provided to help and enter a password in a given sequential order. Pass Points is a click-based cued-recall scheme where a user selects a sequence of points anywhere on an image in deriving a password, and re-selects the same sequence during the authentication when user tries to login the system. Cued Click Points uses one image per click, with the next image selected by a specific random function.

D. *Recognition Based CaRP*

In Recognition based CaRP, a password is an array of visual objects in the alphabet [10], recognition-based CaRP seems to have access to an infinite number of different visual objects.

Fig.1. A ClickText image with 33 characters

Fig.2. Zoo captcha with red circled horses

E. *AnimalGrid based CaRP*

ClickAnimal based CaRP has a smaller alphabet, and a smaller password space than ClickText based CaRP.CaRP should have a large effective password space to resist human guessing attacks. Animal Grids password space can be increased by combining it with a grid-based graphical password, with the grid depending on the size of the selected animal in the given grid.

III. PROBLEM STATEMENT

A. *Existing System*

The existing system relies on CaRP, a new security primitive relying on hard AI problems which cannot be solved easily. CaRP *is* the combination of captcha and graphical password scheme. CaRP introduces a new family of graphical passwords, which adopts a new approach to encounter online guessing attacks [11]. A password of CaRP can be found by automatic online guessing attacks including brute-force attacks, which is having a desired security property that other graphical password schemes do not have. Hotspots in CaRP images can no longer be exploited to mount the automatic online guessing attacks, which is an inherent vulnerability in many graphical

password systems. CaRP forces adversaries to resort to significantly less efficient and much more costlier than human-based attacks. In addition to offering protection from online guessing attacks, CaRP is also used to resist the relay attacks. CaRP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security. The use of CaRP scheme in authentication process is as follows:

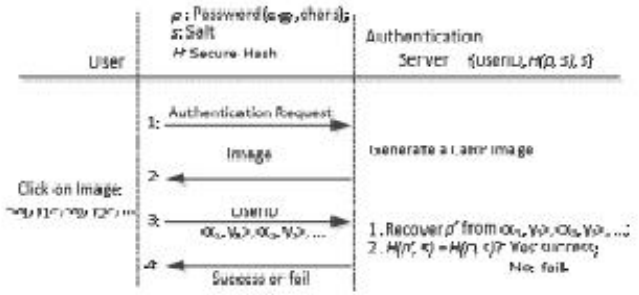

Fig.3. Flowchart Of Basic Authentication

First of all AS stores a salt s and a hash value. For each user ID it stores (,s) where stands for password of count which is not stored and remain secured with the user. Then user send an authentication request to the AS. Upon receiving the login request AS generates a CaRP image and stores the location of the coordinates of the objects in the image and sends the image to the user to click the password whatever the coordinates are selected by the user they are sent to the AS .AS matches the user selected coordinates on the CaRP image the IDs of the object that the user clicked on the image which is recovered back by the AS. Then AS fetches the salt s of the account computes the hash value of with the salt s and compares the result with the hash value of the account . If the two hash values matches then he/she will successfully login the system otherwise login fails.

B. Proposed System

In the existing system security is afforded based on recognition based CaRP where user has to select the appropriate grid of the image as the click points to design a password . Because of which the shoulder surfing attack can be easily arised and the password can be leaked to the third party. So to remove this drawback we are using an advanced secure graphical password in which the user has to go through the two phases :-

1. Registeration Phase
2. Login Phase

Registration Phase

When the user register for the first time he/she has to enter his/her password K of length L characters and select one pointer which will be a default pointer out of given 8 pointers. the user has to register an e-mail address for reenabling his disabled account. The Registration phase should not be working in a Shoulder Surfing environment. In addition, a secure channel should be established between the system and the user during the registration phase . The user's textual password gain by the system from the users entry in password table should be encrypted by the system key.

Login Phase

When the user requests for the login system it displays an image containing different icons the user has to select the correct icons by deriving the pattern within the given specified time (1 sec) if he successfully select the icons within specified time then he will go to the next layer or else fails to login.

In the next layer the image will be displayed in the tabular form in which the group of characters will be present in each block. Whatever the password he had set during the registration phase he will select the correct group of alphabets in which his password is present then internally it will scan and match all the characters which are present in the group if any one of the character matches then it will retrieve the given alphabet which is present in the password likewise it will retrieve all the characters present in the password .

After that an OTP will be sent to the respective email id he/she has to put the key then finally he can successfully login the system.

IV. EXPECTED RESULT

Captcha which is used for graphical password authentication is divided into three modules. The first module has been completed so the expected results based on the first module completion is described with the help of two attributes.

A. Ease Of Use: The proposed system should have better ease of use with less login time resulting in less login attempts which becomes easier for the user and thus providing better security to the user.

B. Robustness : Captcha is robust in nature. In the proposed system the performance remains constant even if error arises in the system but the existing system performmance degrades resulting in loss(data leakage).

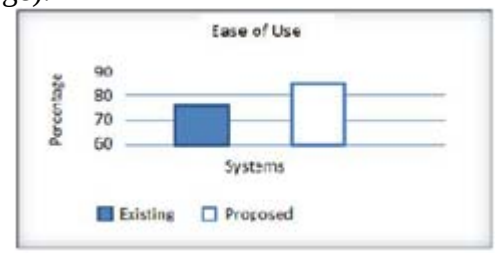

Fig.4 Graph showing ease of use

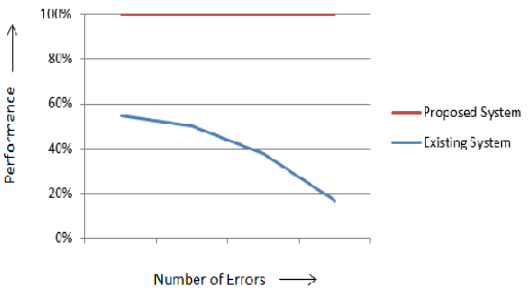

Fig.5 Degree of Performance

V. CONCLUSION

The overall goal of this project is to provide security at the best level. This will improve the performance of online services and prevent from many attacks.. As, this system generates every time a new Captcha challenge at run time it becomes really difficult to guess the password.

ACKNOWLEDGMENT

I would like to thank my guide Prof. Sachin Patil for his personnel involvement, technical guidance, valuable suggestions and continuous consolation throughout the work. Also thank to all authors of papers referred in this paper for their work. It was knowledge gaining and interesting process with best of outcomes.

REFERENCES

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, Captcha as Graphical PasswordsA New Security Primitive Based on Hard AI Problems, IEEE transaction on information forensics and security Vol 9,No. 6 June 2014

[2] I.Jermyn, A. Mayer, F. Monrose, M. Reiter, and A.Rubin,The designand analysis of graphical passwords,in Proc USENIX Security Symp., 1999, pp. 115.

[3] H. Tao and C. Adams, Pass-Go: A proposal to improve the usability of graphical passwords, Int. J. Netw.Security, vol.7, no. 2, pp. 273292 2008

[4] P. C. van Oorschot and J. Thorpe, On predictive models and user drawn passwords, ACM Trans. Inf. Syst.Security,vol. 10, no. 4, pp. 133, 2008

[5] E. Dirik, N. Memon, and J.-C. Birget, Modeling user choice in the passpoints graphical password scheme, in Proc. Symp. Usable Privacy Security, 2007, pp. 2028.J..

[6] K. Golofit, Click passwords under investigation, in Proc.ESORICS, 2007, pp. 343358A.

[7] H. Tao and C. Adams, Pass-Go: A proposal to improve the usability of graphical passwords, Int. J. Netw.Security, voL7, no. 2, pp. 273292, 2008

[8] B. Pinkas and T. Sander, Securing passwords against dictionary attacks, in Proc. ACM CCS, 2002, pp. 161 170

[9] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, PassPoints: Design and longitudinal evaluation of a graphical password system, Int. J. HCI, vol. 63, pp.102127, Jul. 2005

[10] PH TippingPoint DVLabs, Vienna, Austria.(2010). Top Cyber Security Risks Report,SANS Institute and Qualys ResearchLabs[Online].Available:http://dvlabs.tippingpoint.com/toprisks2010

[11] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, CAPTCHA: Using hard AI problems for security, in Eurocrypt, 2003, pp. 294311

[12] R. Biddle, S. Chiasson, and P. C.Oorschot,Graphical passwords: Learning from the first twelve years, ACM Comput. Surveys, vol. 44, no. 4, 2014

[13] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, Influencing users towards better passwords:Persuasive cued click-points, in Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity,Interaction, vol. 1.2008, pp. 121130