CAPTCHA: Hybrid Graphical Passwords as a Robust Multilayer Security Scheme

Prof.Vikhe Prashant B., Sarje Priyanka.M., Pardeshi Karishma k.,Gaikwad Rasika S.

Assistant Professor, Computer Engineering, PREC, Maharashtra, India
Student, Computer Engineering, PREC, Maharashtra, India
Student, Computer Engineering , PREC, Maharashtra, India
Student, Computer Engineering, PREC, Maharashtra, India

ABSTRACT

CAPTCHA is a wordplay for complete Automated Public Turing Test to tell Computer and Human Apart. It addresses a many security problems such as online guessing attacks, relay attacks and combined with dual-view technologies, shoulder-surfing attacks and also hotspot attack. Captcha as graphical passwords (CaRP) is both a Captcha and a graphical password scheme. To address the image hotspot problem in graphical password systems CaRP offers a novel approach such as Pass Points that frequently leads to delicate password choices.

Keyword : - *Graphical password, Dictionary attack, Password guessing attack authentication, Cued click point.*

1. INTRODUCTION

CaRP offer protection against online dictionary attacks on passwords, for various online services which have been for long time a major security threat. This threat is widespread and considered as a top cyber security risk. Safety against online dictionary attacks is a smaller problem than it might appear. Intuitive corrective such as throttling logon attempts do not work for two reasons:

1. It causes denial-of-service attacks.

2. It is vulnerable to global password attacks. The most significant primitive invented is Captcha, which distinguishes from users to computers by presenting a challenge. Standard Internet security technique to protect online email and other services from being abused by bots. Captcha as graphical password is click-based graphical passwords.[1]In click-based graphical passwords unwell chosen passwords give rise to the emergence of hotspots portions of the image where users are more likely to select click-points which allowing attackers to mount more successful dictionary attacks[6].

2. LITERATURE REVIEW

In this a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha , which we call Captcha as graphical passwords.[2] In this paper we review usability requirements for knowledge-based as they apply to graphical passwords, identify security threats. It very hard to remember passwords and PINs yet the human brain effective at the apparently harder task of remembering and recognizing individual faces. In that paper design and analyze graphical password, which can be input by the user to any device with the graphical input interface [3]. In this paper designed a new graphical password scheme, Pass-Go, in this a user selects intersection on a grid as a way to input a password.

2.1 Related work

Captcha is used to protect sensitive user inputs on an untrusted client. This protects the communication key loggers channel between user and Web server from and spyware, CaRP is a family of graphical password for user authentication.

a. Captcha as authentication

The method which we used earlier is a Textual password in which the password which are long is consider as secured password but the long passwords is hard to remember thus the user pick short password but short password are easy to crack .The new technique is which is graphical password and biometric. This technique overcome the shoulder surfing problem in Textual password but these techniques have also some disadvantages like more time for Authentication and it's quite expensive.[1]

b. Captcha

Captcha reals on the gap of capabilities between humans and in solving certain hard AI problems. There are two types of visual Captcha are Text Captcha and Image-Recognition Captcha. [4] The former relies on character appreciation while the latter relies on appreciation of non-character objects. Security of text Captcha antiquated extensively studied.

Fig-1: Textual captcha

The above principle has been established: text Captcha should count on the difficulty of character segmentation, which is computationally expensive and hard. Captcha can be pre mince through relay attacks where by Captcha challenges are relayed for the human solvers whose answers were fed back to targeted application.

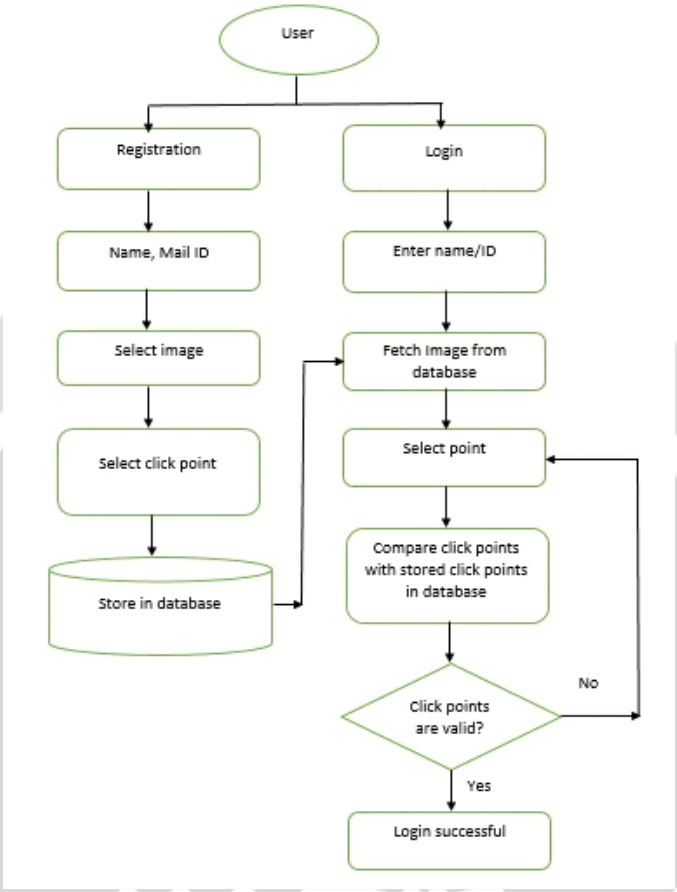
3. PROPOSED METHODOLOGY

In proposed system present a new security primitive based on hard AI problems, a novel family of graphical password systems built on top of Captcha which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password. [1] It addresses a number of security problems combine, such as

1. Online guessing attacks
2. Relay attacks.
3. Shoulder-surfing attacks.
4. Hotspot attack.

By automatic online guessing attacks if the password is in the search set it also offers a novel attend to address the leading image hotspot problem in approved graphical password systems, so Pass Points that often leads to a simple password choices. CaRP is not a panacea it also offers reasonable security and usability and it appears to fit well with some practical applications for improving online Safety **[3].**We exemplary CaRPs built on text Captcha as well as image-recognition Captcha. One of them is a text CaRP where a password is a sequence of characters as like a text password, but to record by clicking the correct character sequence on CaRP images. CaRP offers defense against online dictionary attacks on passwords, which have been for long time a major safety for various online services. This threat is unlimited. Consider as a top cyber safety risk. Defense against online dictionary attacks is a more small problem than it appear.[1]

Our proposed system allow user to select while attempting to influence users to select complicated passwords. It also makes the task of selecting an easy password more tedious, in order to discourage users from making such choices.



.

Fig -2: Flow of CaRP

3.1 Click based graphical password:

Graphical password techniques are a type of information based authentication that attempts to grease the human memory for visual information.[6] Previously pass point techniques used in graphical password in such systems users passwords consist of five click points in sequential manner on a given image. For login purpose user have to remember and repeat that sequence in correct order. To reduce this complications the new technique is invented called as Cued Click Points [7]. Instead of five click points on one image this technique uses single click on single image. Thus remembering the order of the click-points has no longer a requirement on users as the systemcan display only single image at a time.

4. RECOGNITION BASED CARP:

4.1. Click Text:

Click Text is a recognition based CaRP pattern massed on top of transcript captcha. Its alphabet having characters without any visually confusing characters. Suppose, Letter "O" and digit "0" causes confusion in CaRP [6] images and so one character should be eliminated from the alphabet. A Click Text password is an adjustment

of characters in the script for e.g., ρ ="AB#9CD87" which is related to a text password. This is other from text Captcha task in which the characters are mostly ordered from left to right. For users to type them successively a Click Text image having an alphabet of 33 characters.

4.2. Click Animal:

Click Animal is a recognition based CaRP pattern rely on top of captcha Zoo with an alphabet of Alike animals [2] such as cat, monkey, character description is required in a locating points which are clickable on a Text Points image despite the clickable points are well-known to each character. This is a task farther a bot's efficiency.

4.3. Animal Grid:

Number of similar animals is restricted than the number of offered characters. Click Animal has a minor alphabet and so it have a lesser password slot than the Click Text. Animal Grid [1] [3] password space can be enlarged by merging it with a grid based graphical password with the grid amenable on the size of the selected animal.

5. IMPLEMENTATION:

Our captcha engine accepts capital letters, we choose total 33 characters in which all capital letters except I, J, O and Z also all digits except 0 and 1 and three special symbols **#**, **@** and **&** which are used for security balance and user's strong objection of using non alphanumeric characters [1] in the text password.[7]Characters are arranged in 5 rows and each characters are randomly rotated from -30 to +30 and scaled from 60 to 120%. Neighboring characters could overlap up to 3 pixels. Warping effect are set to the light level. Each and every is set to 400 by 400 pixels. For implementing graphical password another technique used is cued click point technique.In this technique password are stored in the form of X, Y co-ordinates on the image [4].

Animals are bird, horse, cow, dog, pig, camel, rabbit, giraffe, element and dinosaur and these animals are arranged in multiple rows and multiple columns, now from each column one image is selected and then one by one each selected image is appeared on screen. We have to select a particular point on that image which is saved in the form of x,y co-ordinates in database. MySQL database connectivity is used here and code is implemented in Java programming language.

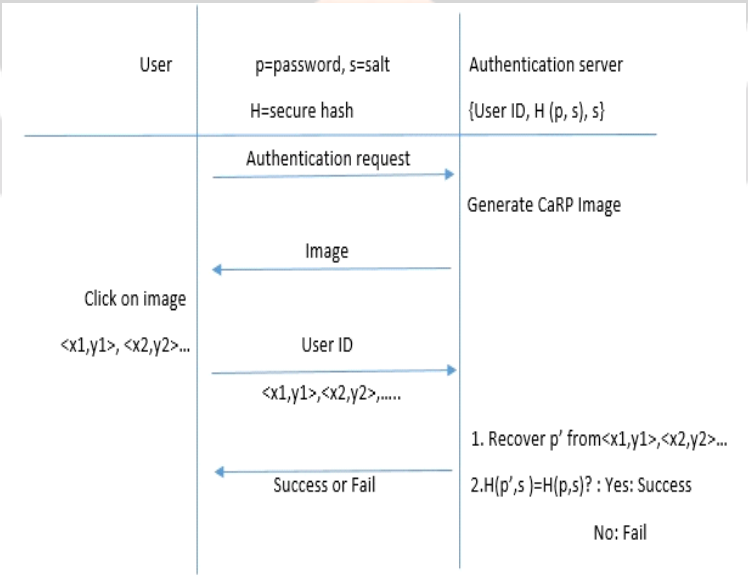


Fig -3: Authentication of user

5.1Algorithm:

There are following steps in this algorithm, there are two levels of authentication.

A] First level of authentication (virtual keyboard):

1. Initialize the all keyboard buttons in the QWERTY pattern.
2. While the key is pressed,
   a. stored all numbers and alphabets in the array.
   b. randomize the all alphabets and numbers in the array.
   c. Reassign the newly formed alphabets and number to the buttons in the array.
   d. Display the characters on the buttons.
   e. if enter key is pressed go to step 3.
3. Check the length of the keys entered in the database.
   if(length = valid)
4. Check for the password match.
   a. If password match go to step 6.
   b. Else go to step 5.
5. Second level of authentication
6. End.

B] Second level of authentication (Graphical password)

1. Registration
   a. Enter user name
   b. Select image
   c. Select cued click points
   d. Points are stored in database in the form of x , y co-ordinates
   e. if enter key is pressed go to step 4.
4. Login
   a. Enter username
   b. Fetch images from database
   c. Click on the points
   d. Compare click points with previously stored points in database
   e. if points are matched the go to step 5
   f. else go to step b
5. Login successful.

6. SECURITY ANALYSIS-

6.1. Security of Underlying Captcha:

Computational effrontery in determine objects in (CaRP) images is fundamental to CaRP [1]. Remaining analysis on Captcha security were mostly used a proper process. A Captcha challenge typically contains 6-10 character where CaRP image mostly contains 30 , more characters .Complexity for breaking a click text image is about $\alpha 30P(N)/(\alpha 10P(N)) = \alpha 20$ times the complexity to crack captcha challenge generated by its lurking captcha method. One of the captcha scheme busted then new and more powerful captcha scheme come out and it can be us to construct new CaRP scheme.

6.2. Automatic Online Guessing Attacks:

In routine online anticipating attacks error process and the trial is performed automatically while dictionaries can be manufactured manually.[4]If the password guess is to be approved in a trial is the confirmed password and the trial has a slim chance to succeed as a machine cannot admit the object in the CaRP image to the password accurately.

6.3. Human Guessing Attacks:

In human predicting attacks the users are knowing enter passwords in the trial and error process. People are much slower than system in increasing guessing attacks. Human guessing attacks on Text Points desired a much longer time than those on Click Text as Text Points has a much longer password space. If we consider that Click Text [6] has approximately the same effective password space like text password and it requires on average 1000 people to work 1.65 days.

6.4. Relay Attack:

Relay attacks are enrolled in different ways. Captcha [4] tasks can be carried out to a high-volume Website hacked are controlled by impedance to have human surfers solve the objection for continue surfing the website or delivered to the sweatshops where users are busy for solving Captcha challenges.

6.5. Shoulder-Surfing Attacks:

When we entered graphical passwords in a public place such as bank ATM machines Shoulder-surfing attacks [2] are a risky. CaRP is not hardy to shoulder surfing attacks by itself.

6.6. Hotspot attack:

Pass points passwords from a small number of users can be used to determine hotspots [5] on an image, which can be used to form an attack dictionary. Up to 36% of passwords on the pool image were accurately guessed with a dictionary words of 231 entries. The attacker's task is more difficult for cued click points because not only is the popularity of hotspots reduced, but also the sequence of images must be determined. [8] Also each relevant image is gather and making a customized attack per user. An online attack could be thwarted by minimizing the number of inaccurate guesses per account.

4. CONCLUSIONS

We have proposed a new security primitive (CaRP) Captcha as graphical passwords relying on unsolved hard AI problem. CaRP is both a captcha as well as graphical password scheme. A password of CaRP can be found only credibility by automatic online guessing attacks. We have discussed concession based CaRP in which Click Text, Click Animal and Animal Grid approaches are included. When one captcha scheme is busted then new and more secure captcha appear which can be converted to CaRP scheme. Also the Cued Click-Point method is very useful and it provides greater security using hotspot technique. Our work is single step forward in the archetype of using hard AI problems for security purpose of sensible security as well as applicability and practical relevance. CaRP has great potential for conversion, which call for important future work. The necessity of CaRP can be more improved by using images at different levels of calamity based on the login review of user as well as the machine which is use for login.

6. REFERENCES

[1].Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, *"Captcha as a graphical password-A new security primptive based on hard AI problem"*, ieee transactions on information forensics and security, vol. 9, No. 6, June 2014

[2].Jayshree Ghorpade, Shamika Mukane, "Devika Patil, Dhanashree Poal, Ritesh Prasad, *"Novel Method for Graphical Passwords using CAPTCHA"*, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4 Issue-5, November 2014

[3].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.

[4].Zhu, B.B., Yan, J., Li, Q., Yang, C., Liu, J., Xu, N., Yi, M., Cai, K. *"Attacks and design of image recognition CAPTCHAs"*, ACM CCS, 187–200 (2010)

[5]/Sonia Chiasson, Alain Forget, Robert Biddle, P.C. van Oorschot,*" Influencing Users Towards Better Passwords:Persuasive Cued Click-Points"*, School of Computer Science,Human-Oriented Technology Lab Carleton University, Ottawa Canada,2008

[6].Ragavendra A., Jeysree J.,*"Graphical password authentication using CaRP"*, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 2, February 2015

[7].M .Swathi, M. V. Jagannatha Reddy,*" Authentication Using Persuasive Cued Click Points"* International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 7, July – 2013.

[8].Lavasnya Reddy L*,K.Alluraiah,*" ECCP: Enhanced Cued Click Point Method for Graphical Password Authentication"*,Volume 3, Issue 8, August 2013.