International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

A Survey Paper on Secure User Authentication using CaRP a security primitive based on Hard AI Problems

Ms Sayali .P Shinde [1], Prof J.S Raghatwan [2]

[1] *ME Student , Department of Computer Engineering, RMDSSOCE ,Warje, Pune, India*

[2] *Assistant Professor, Department of Computer Engineering , RMDSSOCE , Warje, Pune, India*

Abstract *:The major work in security is to use cryptology primitives based on hard mathematical problems that cannot be solved within polynomial amount of time and are usually intractable For eg, the problem of integer factorization of RSA public-key cryptosystem , discrete logarithm problem of Diffie-Hellman key exchange etc. The use of passwords is basic approach used for authentication which has caused threat to computer security ,where passwords are often easy to guess by automated programs running dictionary attacks. In this paper , a scheme is proposed which is based upon click based graphical passwords in which successive taps on a picture is used to deduce password . CaRP as a graphical password offers protection towards various types of attacks on passwords, that is considered as major hazard to security services and considered as a top cyber security risk*

Keywords: **Graphical passwords, password guessing attacks, security primitive, CaRP**

1. INTRODUCTION

The use of hard AI (Artificial Intelligence) problems for security, is being proposed in [16], is interesting and new approach .Under this approach, the most important thing invented is Captcha, where human users and computers are distinguished by presenting a task which is in the form of puzzle where computers are unable to solve it but it is easy for human users to solve it. Captcha has become standard now for various Internet security techniques to avoid attacks on online email and other services from being threatened by intruders

This standard of text based captcha was not up to the mark when results were analyzed with various crypto logical primitives based on hard mathematical problems. So there was need to build new security techniques based on hard AI problems which is challenging task and what we need is optimized solution within polynomial amount of time

To address this issue , a unique approach of graphical password called CaRP which is combination of both text as well as image captcha is proposed. CaRP is tap based graphical password , where successive taps on picture is used to deduce password. CaRP images are captcha challenges and new image is generated for every login process. The idea of CaRP is easy but broad. It can have multiple concretizations. In practice, any captcha scheme depending upon various object classification can be converted into CaRP . Here CaRP can be implemented on both text as well as image - identification captcha. First one is Text CaRP where passphrase is succession of alphabets like text passphrase, but entered by clicking the correct alphabets on successive CaRP pictures.

CaRP provides protective covering against various types of dictionary attacks on pass phrase which has been a long time issue causing harm to different services which are online and this is considered as major threat to cyber security. Defense mechanisms with respect to this online dictionary attacks is major problem and corrective measures should be taken to avoid this. Initially counter measures such as strangling do not work for 2 reasons

1) It causes denial-of-service attacks (causes damage to large number of aspirants in final minutes of eBay

auctions) and incurs expensive help desk costs for account reactivation.

2) It is vulnerable to global password attacks in which intruder causes damage to multiple accounts rather than single on and checks that number of attempts on account does not cross the limit to avoid locking out

CaRP needs to solve a Captcha puzzle for each login attempt

Typical application scenarios for CaRP include:

1) CaRP can be used on touch-screen assets where on typingpassword is very risky especially. for secure Internet transactions such as e-banks. Many banking systems have used scheme of Captchas for their user logins

2) CaRP helps to reduce spam emails by increasing operating cost.

The remaining paper is organized as follows: Background and related work are presented in Section 2. We outline CaRP in Section 3, and present a variety of CaRP schemes in Sections 4. Security analysis is provided in Section 5

2. BACKGROUND AND RELATED WORK

A variety of schemes of graphical password schemes have been implemented They can be categorized into three types into three categories recognition, recall, and cued recall. In recognition-based scheme needs to predict among baits the optical objects belonging to a passphrase in case

Pass faces is a scheme [1] wherein a user ticks from the case of faces stored in database for creating a password. At the time of login a board of applicant faces is presented for the recipient to select the face belonging to her case. This process is repeated for number of turns, each turn with a different board A correct selection in each turn results into successful login. The set of images on board remains the same between logins, but their locations are changed. Story [2] is analogous to Pass faces but the images in the case are ordered, and a user must detect her case images in the right order

Déjà Vu [3] is also same but uses a large set of computerized "random-art" images. Cognitive Authentication [4] requires a recipient to produce a path through a board of images as follows: start from the top-left image, move down if the image is in her case, or right otherwise. This process is repeated, each time with a different board.

A recall-based scheme requires recipient to regenerate the analogous result which should not involve cueing. Draw a secret [5] was the first recall-based scheme proposed. A recipient draws her password on a 2D grid. The system encrypts the sequence of grid cells along the drawing path as password. Pass-Go [6] improves DAS's usability by encrypting grid intersection points instead of grid cells. BDAS [7] adds background images to DAS to motivates users to create more complex password

A cued-recall scheme, help users to memorize and enter a password which is done by exterior cue. Pass Points [8] is a largely studied click-based cued-recall scheme wherein a recipient taps on chain of points anywhere on an image in creating a password, and repeats same taps on image during authentication.

Cued Click Points (CCP) [9] is same as that of Pass Points , instead uses single image per tap, along with the next image chosen by a deterministic function. Persuasive Cued Click Points (PCCP) [10] widens CCP where recipient have to choose a point inside a randomly positioned adjournment in choosing passphrase which results into distributed click-points which are random in a password. Among the three types, recognition is considered the simple for human memory whereas pure recall is the difficult [11]. Recognition is typically the weakest for resistance to attack. There are variety of schemes whose password space is having scope from 2^13 to 2^16 passwords [12]. DAS and Pass-Goare broken easily with guessing attacks. Images contain hotspots[13], [14] in creating passwords. Hotspots were exploited to mount successful guessing attack broken

3. BASIC AUTHENTICATION USING CaRP

3.1 Overview

In order to do login for each attempt of process new image is displayed even if the user is same, it uses character of alphabet of optical objects to generate picture which is puzzle to be solved. The distinguishing things between the images of CaRP and Captcha is that all optical objects in alphabet should be present in CaRP image which will allow recipients to input any pass phrase but there is no necessity of entering it in captcha image . CaRP are graphical passwords which are click-able points. There 2 types of CaRP schemes which are recognition and recognition-recall respectively

In recognition image should be recognized by user and in second case that recognized image is used as cue to create a pass phrase

3.2 CaRP Scheme for User Authentication

CaRP are also provided with additional protection shield between clients and server through transport layer security in which authenticated server stores a hash and salt value given by H(p,s) for every user id in which p is passphrase which is not stored. A CaRP is order of server AS stores a salt s and a hash value H(p, s) for each user ID, where ρ is the password of the account and not stored.

A CaRP password is a set of optical object IDs or clicked points of optical objects that the user selects .When request is received for login attempt server will produce image and will keep record of positions of objects in the image and sends recipient image to click password. The (x,y) positions of image are recorded and sent to server ID of user .Server maps the received (x,y) positions onto CaRP image and recovers a sequence of optical object IDs or clicked points of optical objects p which recipient clicked on image. Server will retrieve salt s of an account and compare result of hash value of particular account. If both hash values match then only login is proceeded further This overall process is basic authentication

4. CaRP SCHEMES

4.1 Click Text Method

Click Text relies on recognition based method which is build on top of text captcha which has characters that are optical which are not confusing. This method has sequence of alphabet characters analogous to text pass-phrase . In this image is generated which is click text by captcha engine which consists of characters of alphabet. When password is created server relies on the ground truth positions of characters clicked by user which are arranged randomly in two dimensional view

Fig.2: Image based upon Click Text

4.2 Click Animal Method

Click Animal is second method based upon a recognition CaRP scheme built on base of Captcha Zoo [15], character alphabet of similar animals such as dog, horse, pig, etc. In this pass phrase is chain of animal names such as ρ = pig , cat ,dog. Then for each of this animal 3D model is produced. In this 3D animals are used to produce 2D animals by using various views, textures, colors, lightning effects, and optionally distortions. The outcome of 2D animals are then placed with untidy background such as grassland. Some animals may be congested by other animals in the image, but their main parts are not congested so that it will be easy for users to predict every animal from it.

Fig.3: Click Animal

4.3 Animal Grid

One of disadvantage of click animal is it provides small password space as it has small alphabets. So to overcome this animal grid is used in which password is based upon the grid and size of grid is based upon animal chosen in click animal method. This particular method is based upon click-a-secret in which recipient clicks on cells of grid to enter a password. In this particular method correct animal must be chosen within the grid , and if it is wrong then it will follow-up wrong sequence of grid.

In order to enter a pass phrase , image of click animal is displayed, and then animal is chosen. This chosen animal appears in n*n grid with rectangle surrounding the chosen animal. Each cell in grid is labeled which will help the users to identify the cell correctly. A user can select the number of cells in grids that matches the password of recipient . As user clicks on animal ,it should match the first animal in his or her password. The (x ,y) coordinates are recorded which are of grid cells and sent to server This process is repeated until the recipient finishes the task of entering password. The sever then recovers the sequence and regenerate the image from animals surrounding rectangle and also recovers the cells of grid which are clicked by user and then hash value which is stored is matched with generated hash value.

Fig. 4: Animal Grid

4.4 Text Points

Text points is another CaRP scheme which is based upon recognition -recall in which recognized image is used as cue to enter password. It is based upon invariant points of object. When entering password , all points which are clickable are marked on characters in CaRP image which will help user choose password. During login attempt recipient will first identify selected characters and choose the points of password on identified characters. The server will map each chosen point selected by user on image, and if it exceeds the tolerable range, then login will not happen. Otherwise stored hash is compared with generated if they match.

Fig.5: Invariant points on image

5. SECURITY ANALYSIS

1. Automatic Guessing attack:

It is computationally difficult to have online guessing attack as object points on CaRP image independent of other CaRP image . So trials in guessing attacks are mutually independent

2. Human Guessing attack:

Humans are used to enter passwords which is based on trial and error process. Also they are much slower than computers in mounting guessing attacks. So it would take several days or thousands of years when system is authenticated using CaRP Schemes

3. Relay attacks :-

There are several ways through which relay attack can be done. In this a person cannot participate in attack unless he is given the amount for the task to be carried out. So a large number of website is hacked and controlled by adversaries. In case of CaRP image used is different from those used in captcha. Because of this it is very difficult or hard for a person to test a password guess by trying to solve captcha challenge.

4. Shoulder surfing attack:-

When combined with dual view technologies above attack can be avoided in which 2 images are displayed simultaneously ,in which one of them is public and can be viewed from all angles, and other is private image which can be viewed at specific angle. So that it is possible for attacker to view all user-clicked points on public image while it is not possible for private CaRP image . Thus captured points are useless for next login attempt.

6. CONCLUSIONS

Picture password authentication is click based graphical authentication scheme which is used to overcome drawbacks of traditional systems. This authentication process will allow to store the database of users and it will be in the form of image clicks by user. Click based graphical password scheme provides protection against various types of online dictionary attacks and relay attacks, human guessing attacks which have been for long time a major security threat for various online services.

ACKNOWLEDGEMENT

I like to acknowledge my gratitude to Prof. J.S. Raghatwan for valuable suggestions in carrying my research work. I also take opportunity to thank my friends for supporting me

REFERENCES

[1] (2012, Feb.). *The Science Behind Passfaces* [Online]. Available:http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[2] D. Davis, F. Monrose, and M. Reiter, "On user choice in graphicalpassword schemes," in *Proc. USENIX Security*, 2004, pp.1–11.

[3] R. Dhamija and A. Perrig, "Déjà Vu: A user study using images for authentication," in *Proc. 9th USENIX Security*, 2000, pp. 1–4.

[4] D. Weinshall, "Cognitive authentication schemes safe against spyware," in *Proc. IEEE Symp. Security Privacy*, May 2006, pp. 300–306

[5] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th USENIX Security Symp.*, 1999, pp. 1–15.

[6] 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. 273–292, 2008.

[7] P. Dunphy and J. Yan, "Do background images improve 'Draw a Secret' graphical passwords," in *Proc. ACM CCS*, 2007, pp. 1–12.

[8] 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. 102–127, Jul. 2005

[9] 9]S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Proc. ESORICS*, 2007, pp. 359–374.

[10] [10] 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. 121–130.

[11] [11] 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.

[12] [12]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. 273–292, 2008.

[13] [13]K. Golofit, "Click passwords under investigation," in *Proc. ESORICS*, 2007, pp. 343–358.

[14] [14] A. 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.20–28.

[15] R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, "A new CAPTCHA interface design for mobile devices," in *Proc. 12th Austral. User Inter. Conf.*, 2011, pp. 3–8.

[16] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in *Proc. Eurocrypt*, 2003, pp.294–311.

[17] J. Elson, J. R. Douceur, J. Howell, and J. Saul, "Asirra: A CAPTCHA that exploits interest-aligned manual image categorization," in *Proc. ACM CCS*, 2007, pp. 366–374.

[18] 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.

[19] N. Joshi. (2009, Nov. 29). *Koobface Worm Asks for CAPTCHA*[Online].Available:http://blogs.mcafee.com/mcafee-labs/koobface-worm-asksfor- CAPTCHA

[20] M. Szydlowski, C. Kruegel, and E. Kirda, "Secure input for web applications," in *Proc. ACSAC*, 2007, pp. 375–384.

[21] 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.

[22] Bin B. Zhu, Je_ Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "Captcha as Graphical Passwords |A New Security Primitive Based on Hard AI Problems" ,in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE

BIOGRAPHIES

Ms Sayali Shinde has Bachelor degree in information technology from Rajarambapu Institute of Technology, Shivaji University. Currently pursuing post graduation in computer engineering from Pune University. Area of interests are security, data mining.)

Prof.Jyoti Raghatwan has master degree in information technology from Pune University. She has 7 years of experience in teaching field. Currently working as Assistant Professor at RMDSSOCE ,Warje Pune. Her area of interest is information security