Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Authentication Using CAPTCHA as Graphical Password

M. M. Vamsi Priya[1], Sushma Nallamalli[2], D. Bhanu Prakash[3], K. Ramya Sri[4]
[1, 3] Assistant Professor, [2] Associate Professor, [4] B.Tech Graduate
[1, 2, 3, 4] Department of CSE, DMSSVH College of Engineering,
Machilipatnam (AP), India

Abstract--Cyber security is an important issue to tackle. Various user authentication methods are used for this purpose. It helps to avoid misuse or illegal use of highly sensitive data. Text passwords have been widely used for user authentication, But due to various flaws, they are not reliable for data security. Graphical password schemes are believed to be more secure and more resilient to dictionary attacks than textual passwords, but more vulnerable to shoulder surfing attacks. Many recognition-based graphical password schemes alone, in order to offer sufficient security, require a number of rounds of verification, introducing usability issues. In this paper we suggest a new hybrid user authentication approach combining CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) and graphical passwords to provide increased security. We call it as CAPTCHA as gRaphical Password (CaRP).In this paper we conduct a comprehensive survey of existing CaRP techniques namely ClickText, ClickAnimal and AnimalGrid. We discuss the strengths and limitations of each method and point out research direction in this area by performing the security analysis.

Keywords: CAPTCHA, CaRP, Graphical Passwords, User Authentication, Security.

I. INTRODUCTION

Today, authentication is the principal method to guarantee information security and the most common and convenient method is password authentication [2].Traditional alphanumeric passwords are strings of letters and digits, which are easy and familiar to all users. However, there are several inherent defects and deficiencies in alphanumeric passwords, which easily evolve into security issues. Due to the limitation of human memory, most users tend to choose short or simple passwords which are easy to remember [3]. Surveys show that frequent passwords are personal names of family members, birth date, or dictionary words. In most cases, these passwords are easy to guess and vulnerable to dictionary attack [4], [5]. Today users have many passwords for personal computers, social networks, E-mail, and more. They may decide to use one password for all systems to decrease the memory burden, which reduces security [6], [7]. Moreover, alphanumeric passwords are vulnerable to shoulder surfing attack, spy ware attack and social engineering attack etc. Motivated by the promise of improved password usability and security, the concept of graphical passwords was proposed in 1996 [8]. Like alphanumeric passwords, graphical passwords are knowledge-based authentication mechanisms. The main goal of graphical passwords is to use images or shapes to replace text, since numerous cognitive and psychological studies demonstrated that people perform far better when remembering pictures than words [9]. The most widely accepted theory explaining this difference is the dual-coding theory [9], suggesting that verbal and non-verbal memories are processed and represented differently in the mind. Assigned with perceived meaning based on direct observation, the images are represented in a way that retains the perceptual features being observed. The text is represented with symbols that convey associatively cognitive meaning. As a result, additional processing required for verbal memory renders a more difficult cognitive task. Thus it is easy for human being to remember faces of people, places they visit and things they have seen for a lengthy duration.

A Captcha is a program that can generate and grade tests that: (A) Most humans can pass, but (B) Current computer programs can't pass. A Captcha is a cryptographic protocol whose underlying hardness assumption is based on an AI problem. Such a program can be used to differentiate humans from computers and has many applications for practical security, including (but not limited to):

-Online Polls: In November 1999, slashdot.com released an online poll asking which was the best graduate school in Computer Science (a dangerous question to ask over the web!). As is the case with most online polls, IP addresses of voters were recorded in order to prevent single users from voting more than once. However, students at Carnegie Mellon found a way to stuff the ballots by using programs that voted for CMU thousands of times. CMU's score started growing rapidly. The next day, students at MIT wrote their own voting program and the poll became a contest between voting"bots". MIT finished with 21,156votes, Carnegie Mellon with 21,032 and every other school with less than 1,000.Can the result of any online poll be trusted? Not unless the poll requires that only humans can vote.

-Free Email Services: Several companies (Yahoo!, Microsoft, etc.) offer free email services, most of which suffer from a specific type of attack:" bots" that sign up for thousands of email accounts every minute. This situation can be improved by requiring users to prove they are human before they can get a free email account.Yahoo!, for instance, uses a Captcha to prevent bots from registering for accounts. Their Captcha asks users to read a distorted word such as the one shown below (current computer programs are not as good as humans at reading distorted text).

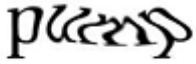

Fig. 1. The Yahoo! CAPTCHA.

***-Search Engine Bots*:** Some websites don't want to be indexed by search engines. There is a html tag to prevent search engine bots from reading webpages, but the tag doesn't guarantee that bots won't read the pages; it only serves to say "no bots, please". Search engine bots, since they usually belong to large companies, respect webpages that don't want to allow them in. However, in order to truly guarantee that bots won't enter a web site, Captcha's are needed.

***-Worms and Spam*:** Captcha's also offer a plausible solution against email worms and spam: only accept an email if you know there is a human behind the other computer. A few companies, such as www.spamarrest.com are already marketing this idea.

***-Preventing Dictionary Attacks*:** Pinkas and Sander have suggested using Captcha's to prevent dictionary attacks in password systems. The idea is simple: prevent a computer from being able to iterate through the entire space of passwords by requiring a human to type the passwords.

CAPTCHA standing for "Completely Automated Public Turing test to tell Computers and Humans Apart", is an automatic challenge-response test to distinguish between humans and machines [12].Captcha is used for protection against different attack i.e. bot. In image based, Captcha is click based graphical passwords, where sequence of clicks on an image is used to derive a password. It provides protection against online dictionary attacks on password. In this for login every time click on images. Captcha can be applied on touch screen devices where on typing passwords is not more secure, especially for secure internet applications such as e-banks. For example ICBC (www.icbc.com.cn) used Captcha. This bank is largest bank in world for every login user has to solve Captcha challenges. Captcha helps to reduce spam emails [1].In early system only text password is used which is very difficult to remember if it is a long password. If we use smaller password then it can be easily identified and we also use common password for many accounts so for that Image based Captcha provide more security during authentication.

CaRP is a combination of both a CAPTCHA and a graphical password scheme. CaRP overcome a number of security issues, such as relay attacks, online guessing attacks, and, if combined with CAPTCHA and graphical password, shoulder-surfing attacks. CaRP is click-based graphical passwords, where order of clicks on an image is used to get a new password. Unlike other click-based graphical passwords, images used in CaRP are used to generate CAPTCHA challenges, and for every login attempt a new CaRP image is generated whether the existing user tries authenticating or a new user. In this paper we conduct a comprehensive survey of existing CaRP techniques namely ClickText, ClickAnimal and Animal Grid. We point out research direction in this area. We also try to answer our CaRP as secured as graphical passwords and text based passwords. Survey will be useful for information security researchers and practitioners who are interested in finding an alternative to graphical authentication methods.

II. LITERATURE SURVEY

2.1 CAPTCHA

A CAPTCHA is a program that can generate and grade tests that most humans can pass, but current computer programs cannot pass. Captcha finds the difference between humans and bots in solving the hard AI problems. Such a program can be used to differentiate humans from computers [1]. There are two types of visual CAPTCHA: Text Captcha which is recognition of non-character objects and Image Recognition Captcha(IRC) relies on recognition of images [13].CAPTCHA can be circumvented through relay attacks whereby CAPTCHA challenges are relayed to human solvers [1].

2.1.1 Text Captcha

PayPal and Microsoft Captcha are both relied on background noise and random character strings to resist automated attacks. The Captchas used by Google, Yahoo! all share similar properties: such as a lack of background noise, distortion of characters or word images and extreme crowding of adjacent character. The human readability of random Captcha images is captured by site in the form of pixel, marginal probabilities and site by site covariance [13]. EZ-Gimpy uses word images which employ character distortion and clutter. Pessimal Print uses a low quality images by degrading parameters to thicken, crowd, fragment and add noise to character images. These Captcha's are shown in Fig.2.

Fig.2 Some CAPTCHA Styles

2.1.2 Image Recognition Captcha

These Captcha consist of combination of images. User has to recognize the images given to him to solve the given puzzle. As shown in Fig. 3 user has to select the cat images as the password characters.

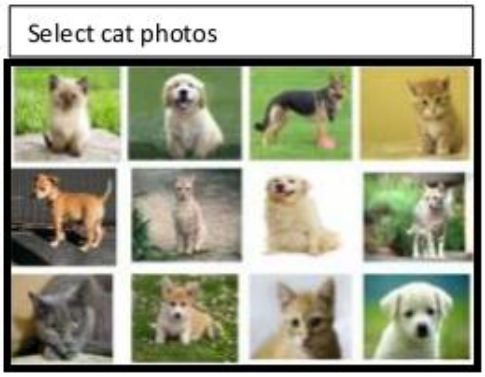

Fig 3.Image Based Captcha

2.2 GRAPHICAL PASSWORD

Graphical Password was originally defined by Blonder (1996).Graphical password schemes have been proposed as a possible alternative to alphanumeric schemes, motivated partially by the fact that humans can remember images easily than text; psychological studies supports such assumption. Images are generally easier to be remembered than text. In addition, if the number of possible images is enough large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer better resistance to dictionary attacks. Because of these (presumed) advantages, there is a increasing interest in graphical password. In addition to web log-in applications and workstation, graphical passwords have also been applied to mobile devices and ATM machines.

A Graphical Password system is of three types as:

1. Recognition Based scheme
2. Recall Based scheme
3. Cued Recall Based scheme

2.2.1 Recognition Based scheme

A recognition based scheme identifies among group of visual objects belonging to a password portfolio. Passfaces is the most widely used scheme. Where a user selects a portfolio of faces from a database in creating a password. While authentication, a panel of candidate faces is presented for the user to select the face belonging to his portfolio. This process is repeated several rounds, with a different panel for each round. Correct selection in each round tends to successful login. In Cognitive Authentication user generate a path through a panel of images –starting from the top left image ,moving down if the image is the portfolio, or right otherwise. The other way round is a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he selected during the registration stage.

2.2.1 Recall Based scheme

In recall based scheme user has to regenerate the same interaction result without cuing (i.e.) a user is asked to reproduce something that he/she created or selected earlier during registration phase. Draw-A-Secret is the well known scheme. A 2D grid is provided to draw a password. The system encodes the sequence of grid cells along the drawing path. Pass-Go is another integrated version of DAS where grid intersections are encoded instead of grid cells.

2.2.3 Cued Recall Based scheme

Pass Points 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 click at the same points as the password. Cued Click Points (CCP) is another scheme where one image per click is used. Persuasive Cued Click Points (PCCP) extends CCP where user has to select a point inside a randomly positioned viewport.

III. CAPTCHA AS GRAPHICAL PASSWORD

Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu [1] proposed CaRP scheme. In CaRP i.e. CAPTCHA as gRaphical Passwords, CAPTCHA and graphical password is combined and used as a single entity for authentication. CaRP is click based graphical password system, where a sequence of click on images is used to define a password. CaRP can be used in:

1. CaRP can be applied on touch screen devices for typing password for secure banking application.
2. CaRP increases spammer's operating cost and thus helps reduce spam emails. An email service provider who deploys CaRP, a spam bot cannot log into an account even if it knows the password. Human involvement is necessary to access an account.

The CaRP schemes are actually click-based graphical passwords with the CAPTCHA technique used in a way that a new image is generated for every login attempt even for the existing user just as Captcha's change every time. CaRP uses an alphabet set. Instead of actual characters, visual objects i.e. a visual depiction of alphanumeric characters or might be some objects is used for the CaRP image generation which actually turns out to be a CAPTCHA challenge. Noticeable difference between normal CAPTCHA and CaRP images is that all objects of an alphabet set for a CaRP scheme are included in every image challenge unlike normal Captcha's where only a part of alphabet set is used. Many CAPTCHA schemes can be converted to CaRP schemes, as described in the next subsection.

On the basis of the memory tasks in memorizing and entering a password, classification of CaRP schemes can be done as follows: recognition based and recognition-recall. The second scheme i.e. recognition – recall CaRP is a new category which works by recognizing an image and using the recognized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition and cued-recall. It retains the advantages of both schemes i.e. recognition advantage of being easy for human memory and the cued-recall advantage of a large password space.

3.1 Authentication process in CaRP Schemes

A CaRP password is a sequence of visual objects IDs or clickable points of visual objects that user selects. The authentication server AS stores a salt s and hash value H (p, s) for each user where p is the password. When a user attempts to login, AS generate a CaRP image, records the locations of the objects in the image, and sends the image to the user to click the password. The clicks coordinates are recorded and passed to AS along with user ID. AS matches the received co-ordinates onto a CaRP image which user clicked with the clickable points of visual objects of p. Then AS retrieves salt s of the account, calculates the hash value of p with the salt, and compares the result with the hash value stored for the account. If the two hash value matches, it means that the authentication is successful. The above explained CaRP authentication process can be shown diagrammatically in Fig 4 and algorithm representation is:

Step 1: Enter ID and send it to Authentication server AS.
Step 2: AS Stores a salt and hash value H(p, s) for each ID.p is the user password and it is stored.
Step 3: Upon receiving login request, AS generates a CARP image. It records location of characters or animals in image and the image is sent to the user.
Step 4: User Clicks the Password.
Step 5: Co-ordinates of points are recorded are sent to AS.
Step 6: AS maps these Co-ordinates & recovers clickable points of object p, that user clicked.
Step 7: Then AS retrieves salt s of account &calculate its hash value with salt using algorithm like SHA-1.
Step 8: IT compares result with hash value stored for the a/c.
Step 9: Authentication is successful if and only if the two hash value matched

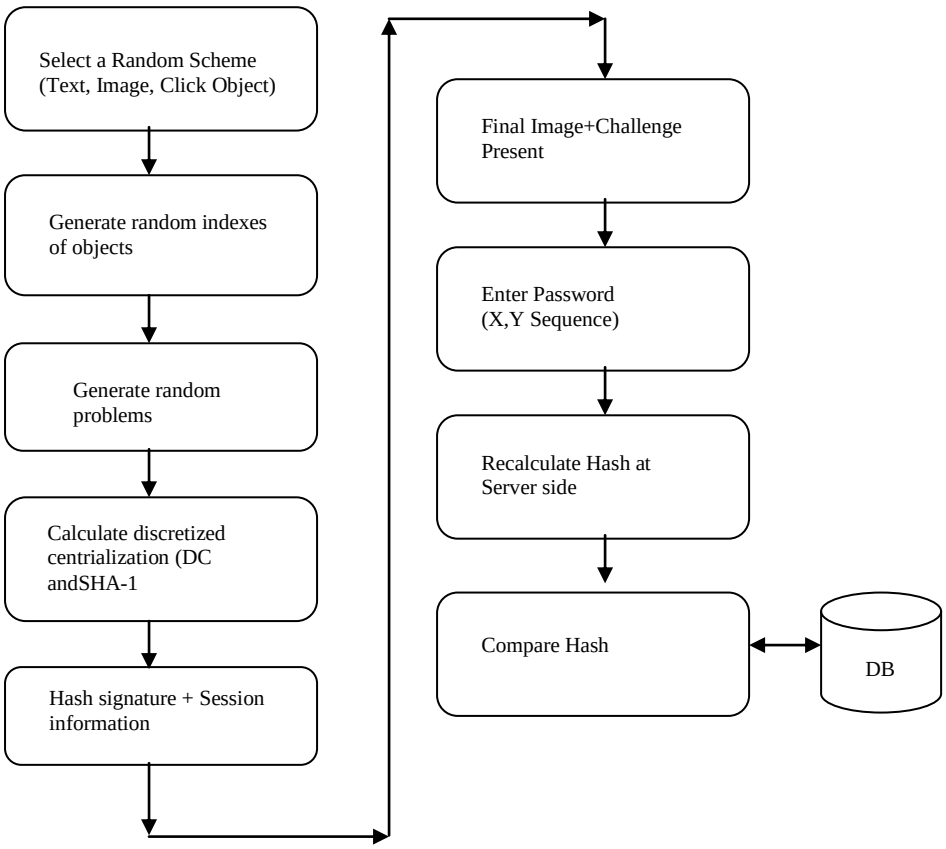

Fig. 4. Flowchart of Basic CaRP Authentication.

3.2 RECOGNITION BASED CaRP

For this type of CaRP, a password is a sequence of visual objects in the alphabet. Per view of traditional recognition based graphical passwords, recognition-based CaRP seems to have access to an infinite number of different visual objects. We present three recognition-based CaRP schemes and a variation next.

3.2.1 CLICKTEXT

Fig 5. Click Text image with 33 characters

ClickText is a recognition-based CaRP scheme built on top of text Captcha. It uses text CAPTCHA as its underlying principle. Alphabet set of ClickText comprises alphanumeric characters. Its alphabet comprises characters without visually-confusing characters. For example, Letter "O" and digit "0" may cause confusion in CaRP images, and thus one character should be excluded from the alphabet. A ClickText password is a sequence of characters in the alphabet e.g., ρ ="DE@F2SK78", which is similar to a text password.. A ClickText image is different from usual CAPTCHA as here all the characters of alphabet set are to be included in the image as shown in Fig.5. Generally in this method 33 Capital Letters except I, J, O, and Z digits except 0 and 1, and three special characters #,@,and &.The last three characters is used to balance the security. Characters were arranged in 5 rows. Each character was randomly rotate from -30 degree to 30 degree and scaled from 60% to 120%.Neighboring characters could overlap up to 3 pixels.

A ClickText image is generated by the underlying Captcha engine as if a Captcha image were generated except that all the alphabet characters should appear in the image. During generation, each character's location is tracked to produce ground truth for the location of the character in the generated image. The authentication server relies on the ground truth to identify the characters corresponding to user-clicked points.In ClickText images, characters can be arranged randomly on 2D space. This is different from text Captcha challenges in which characters are typically ordered from left to right in order for users to type them sequentially. In entering a password, the user clicks on this image the characters in her password, in the same order. When image is generated, each character's location in the image is recorded which would be used in authentication

3.2.2 CLICKANIMAL

Fig 6.Click Animal image with Horse Circled 'red'

Captcha Zoo is a Captcha scheme which uses 3D models of horse and dog to generate 2D animals with different textures, colors, lightings and poses, and arranges them on a cluttered background. A user clicks all the horses in a challenge image to pass the test. Fig.5 shows a sample click image challenge with 10 animals wherein all the horses are circled red. ClickAnimal is a recognition-based CaRP scheme built on top of Captcha Zoo , with an alphabet of similar animals such as dog, horse, pig, etc. Its password is a sequence of animal names such as ρ = "Turkey, Cat, Horse, Dog,…." For each animal, one or more 3D models are built. The Captcha generation process is applied to generate ClickAnimal images: 3D models are used to generate 2D animals by applying different views, textures, colors, lightning effects, and optionally distortions. The resulting 2D animals are then arranged on a cluttered background such as grassland. Some animals may be occluded by other animals in the image, but their core parts are not occluded in order for humans to identify each of them. The number of similar animals is much less than the number of available characters. ClickAnimal has a smaller alphabet, and thus a smaller password space, than ClickText [1].

3.2.2 ANIMAL GRID

Fig 7. Click Animal images (left) and 6x6 grid (right)

In order to resist human guessing attacks, a sufficiently-large effective password space should be present for CaRP schemes. If the ClickAnimal scheme be combined with grid-based graphical passwords, its password space can be increased. The grid can be made depending on the size of the selected animal. For authentication process, a ClickAnimal image is displayed first. After an animal is selected, an image of n×n grid appears, with the grid-cell size equaling the bounding rectangle of the selected animal. Each grid-cell is labeled to help users identify. It has the advantage that a correct animal should be clicked in order for the clicked grid-cell(s) on the follow-up grid to be correct. If a wrong animal is clicked, the follow-up grid is wrong. A click on the correctly labeled grid-cell of the wrong grid would likely produce a wrong grid-cell at the authentication server side when the correct grid is used. In the given example 10 animals are used: bird, cow, horse, dog, giraffe, pig, rabbit, camel, elephant and dinosaur. Each animal had three 3d models.3d animal model was randomly selected and posed at a random view in generating a 2d object. Each click animal image was also set to 400 by 400 pixels. A 6x6 grid was used for CAS. Cells were labeled clockwise starting from cell 0.

The process of entering password is follows. . . A ClickAnimal image is displayed first. When user selects an animal, an image of n X n grid is displayed with the grid cell size equaling the bounding rectangle of the selected animal. Fig. 7 shows a 6 X 6 grid. A user can select zero or multiple grid cells matching her password. So, the password is a series of animals interleaving with grid cells. E.g. "Dog, Grid_2, Grid_1,Cat,Horse,Grid_3" where Grid_1 means the grid cells indexed as 1.Grid cells after an animal means that grid is determined by bounding rectangle of the animal. When a ClickAnimal image is displayed , the user selects the animal matching the first animal from the password by clicking on the animal. The clicked point's coordinates are recorded. The bounding rectangle is calculated and displayed. E.g. white rectangle in fig 7. The user corrects the inaccurate edges if any by dragging it. This process is repeated until user satisfaction. After this an image of nXn grid for the bounding rectangle is displayed. Now the user selects a sequence of zero or multiple grid cells that match with grid cells following the first animal in the password, and the go back to ClickAnimal image. The above specified password will result in the sequence as "AP_150,50,GP_30,40,GP_53,130,AP_120,89……" where "AP_x,y" denotes the points of ClickAnimal Image, and "GP_x,y" denotes the points on a grid image. These coordinates are sent to authentication server.

IV. SECURITY ANALYSIS

4.1 Security of Underlying Captcha:

ClickText is much harder to break than its underlying Captcha scheme. Furthermore, characters in a CaRP scheme are arranged two dimensionally, further increasing segmentation difficulty due to one more dimension to segment. As a result, we can reduce distortions in ClickText images for improved usability yet maintain the same security level as the underlying text Captcha. ClickAnimal relies on both object segmentation and multiple-label classification. Its security remains an open question. As a framework of graphical passwords, CaRP does not rely on any specific Captcha scheme. If one Captcha scheme gets broken, a new and more robust Captcha scheme may appear and be used to construct a new CaRP scheme. In the remaining security analysis, we assume that it is intractable for computers to recognize any objects in any challenge image generated by the underlying Captcha of CaRP.

Usually a CAPTCHA challenge might contain about 5 to 8 characters. A CaRP image on the other hand might contain about 30 or more characters. The complexity to break a Click-Text image is about 20 times the complexity to break a CAPTCHA challenge generated by its underlying CAPTCHA scheme[1]. Thus we can get to the conclusion that the CaRP ClickText image is much harder to break than its underlying CAPTCHA scheme. As a framework of graphical passwords, CaRP does not rely on any specific CAPTCHA scheme. If one CAPTCHA scheme is broken, a new and more robust CAPTCHA scheme may appear and be used to construct a new CaRP scheme.

4.2 Automatic Online Guessing Attacks:

The trial and error process is executed automatically in automatic online guessing attacks. However, dictionaries can be constructed manually. Such attacks can find a password only probabilistically without considering the number of trials. If a password guess in the trials is the correct one, the trial still has a lower

chance of succeeding because a machine might not recognize the objects of CaRP in order to enter the correct password. This is different than the online guessing attacks on existing deterministic graphical passwords where each trial can determine if the tested password guess is the correct password or not. Also, with targeted passwords in the dictionary, attacking existing graphical passwords is successful for brute-force or dictionary attacks. If we ignore negligible probabilities, CaRP with underlying CPA-secure.

4.3 Human Guessing Attacks

In human guessing attacks, humans are used to enter passwords in the trial and error process. Humans are much slower than computers in mounting guessing attacks. For 8-character passwords, the theoretical password space is $338 \approx 240$ for ClickText with an alphabet of 33 characters, $108 \approx 226$ for ClickAnimal with an alphabet of 10 animals, and $10 \times 467 \approx 242$.

4.4 Relay Attacks:

Relay attacks may be executed in several ways. Captcha challenges can be relayed to a high-volume Website hacked or controlled by adversaries to have human surfers solve the challenges in order to continue surfing the Website, or relayed to sweatshops where humans are hired to solve Captcha challenges for small payments.

4.5 Shoulder-Surfing Attacks

Shoulder-surfing attacks are a threat when graphical passwords are entered in a public place such as bank ATM machines. CaRP is not robust to shoulder-surfing attacks by itself. However, combined with the following dual-view technology, CaRP can thwart shoulder-surfing attacks.

4.6 Others

CaRP is not bulletproof to all possible attacks. CaRP is vulnerable if a client is compromised such that both the image and user-clicked points can be captured. Like many other graphical passwords such as CCP and PCCP, CaRP schemes using the basic CaRP authentication are vulnerable to phishing since user-clicked points are sent to the authentication server.

4.7 CaRP vulnerable to relay attacks?

There are various ways to carry out relay attacks. Considering CAPTCHA challenges on websites to be hacked, one way of attack is to have human surfers solve the challenges to continue surfing the Website. Another way is having relayed to sweatshops where humans are hired to solve CAPTCHA challenges given small payments. The task to perform and the image used in CaRP are very different from those used to solve a CAPTCHA challenge. This noticeable difference makes it hard for a person to mistakenly help test a password guess by attempting to solve a CAPTCHA challenge. Therefore it would be unlikely to get a large number of unwitting people to mount human guessing attacks on CaRP. In addition, human input obtained by performing a CAPTCHA task on a CaRP image is useless for testing a password guess [1].

V. CONCLUSION

The paper conducts a comprehensive survey of CAPTCHA as Graphical Password schemes which will be a new Security primitive relying on unsolved hard AI problems. CaRP is both a Captcha and a graphical password scheme. As it is combination of both Captcha and Graphical password it makes it very hard to guess the password to the intruders or bots. Effective use of both the techniques makes it useful to use it for smartphones and computers accessing the secure applications such banking, mailing ,etc. CaRP schemes are classified as Recognition-Based CaRP and Recognition-Recall CaRP. We have discussed Recognition-Based CaRP which include ClickText, ClickAnimal and AnimalGrid techniques in this paper. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks. CaRP forces adversaries to resort to significantly less efficient and much more costly human-based attacks. In addition to offering protection from online guessing attacks, CaRP is also resistant to Captcha relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. CaRP can also help reduce spam emails sent from a Web email service. In the implemented module a CaRP image for particular user will get generated. User can sign up by giving his/her username and password. Password is displayed in CaRP image which is combination of password characters and non-password characters.

Current graphical password techniques are an alternative to text password but are still not fully secure. As a framework, CaRP does not rely on any specific CAPTCHA scheme. When one CAPTCHA scheme is broken, a new and more secure one may appear and be converted to a CaRP scheme. Due to reasonable security and usability and practical applications, CaRP has good potential for refinements. The usability of CaRP can be further improved by using images of different levels of difficulty based on the login history of the user and the machine used to log in.Various CAPTCHA alternatives are continuously emerging, and this race will continue as more advanced bots emerge. However, the basic idea of CAPTCHAs is to tell humans and machines apart, and this concept is still worth to be discovered for several reasons. Future trends in CAPTCHA techniques henceforth need to encourage the application of AI-hard problems for efficient prevention of bots.

REFERENCES

[1] Bin B.Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu. Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems. IEEE TRANSACTIONS ON INFORMATION FORENSIS AND SECURITY, VOL.9, NO 6, June 2014.

[2] K. Renaud. "Evaluating authentication mechanisms". In L.Cranor and S. Garnkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6, pp.103-128. O'Reilly Media, 2005.

[3] A. Adams and M. A. Sasse. "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures". Communications of the ACM, 42:41-46, 1999.

[4] D. Florencio and C. Herley. "A large-scale study of WWW password habits". In 16th ACM International World Wide Web Conference (WWW) , May 2007.

[5] A. Adams, M. A. Sasse, and P. Lunt. "Making passwords secure and usable". In HCI 97: Proceedings of HCI on People and Computers, pp.1-19, London, UK, 1997. Springer-Verlag.

[6] G. Blonder. "Graphical passwords". United States Patent, 5,559,961, 1996.

[7] B. Kirkpatrick. "An experimental study of memory". Psychological Review , 1:602-609, 1894

[8] S. Madigan. "Picture memory". In J. Yuille, editor, Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio, chapter 3, pp.65-89. Lawrence Erlbaum Associates, 1983.

[9] A. Paivio, T. Rogers, and P. C. Smythe. "Why are pictures easier to recall than words?", Psychonomic Science, 11(4):137-138, 1968.

[10] Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford, "CAPTCHA: Using Hard AI Problems For Security"

[11] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen, "Graphical Passwords: A Survey", Department of Computer Science Georgia State University.

[12] Hossein Nejati, Ngai-man Cheung, Ricardo Sosa and Dawn C.I.Koh. DeepCaptcha: An Image CAPTCHA Based on Depth Perception. ACM digital Library, March 2014.

[13] Michael A. Kouritzin*, Fraser Newton, And Biao Wu, " On Random Field Captcha Generation"

