ISSN:0975-9646

CAPCHA as Graphical Password

1.**Magniya Davis**
Computer science Department, Calicut University
Kerala, India

2.**Divya R**
Asst. Professor,Computer science Department
Sahrdaya College of Engineering and Technology

3.**Vince Paul,**
HOD,Computer science Department
Sahrdaya College of Engineering and Technology

4.**Sankaranarayanan P N,**
Asst. Professor, Computer science Department
Sahrdaya College of Engineering and Technology

Abstract — The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, user tends to pick a passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. In this paper, we conduct a comprehensive survey of the existing graphical password techniques and captcha. Using hard AI problems for security is emerging as an exciting new paradigm, but has been under-explored. In this paper, we present a new security primitive based on hard AI problems, graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme .We discuss the strengths and limitations of each method and point out the future research directions in this area. And also major design and implementation issues are clearly explained. The main advantage of this method is it is difficult to hack.

Keywords—Graphical password , password, CaRP, Captcha, dictionary attack, password guessing attack, security primitive.

I. Introduction

The most common computer authentication method is for a user to submit a user name and text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username password authentication, alternative authentication methods, such as biometrics have been used. However, we will focus on another alternative, using pictures as passwords.

Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots.However, this new paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. Is it possible to create any new security primitive based on hard AI problems? This is a challenging and interesting open prob-lem. In this paper, we introduce a new security primitive based on hard AI problems, namely, a novel family of graphical pass-word systems integrating Captcha technology, which we call CaRP (Captcha as gRaphical Passwords). CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt.The notion of CaRP is simple but generic. CaRP can have multiple instantiations. In theory, any Captcha scheme relying on multiple-object classification can be converted to a CaRP scheme.

CaRP requires solving a Captcha challenge in every login. This impact on usability can be mitigated by adapting the CaRP image's difficulty level based on the login history of the account and the machine used to log in.

Typical application scenarios for CaRP include:

1) CaRP can be applied on touch-screen devices whereon typing passwords is cumbersome, esp. for secure Internet applications such as e-banks. Many e-banking systems have applied Captchas in user logins. For example, ICBC (www.icbc.com.cn), the largest bank in the world, requires solving a Captcha challenge for every online login attempt.

CaRP increases spammer's operating cost and thus helps reduce spam emails. For an email service provider that deploys CaRP, a spam bot cannot log into an email account even if it knows the password. Instead, human involvement is compulsory to access an account. If CaRP is combined with a policy to throttle the number of emails sent to new recipients per login session, a spam bot can send only a limited number of emails before asking human assistance for login, leading to reduced outbound spam traffic.

II. Background works

Authentication is the process to allow users to confirm his or her identity to a Web application. Human factors are often considered the weakest link in a computer security system. Point out that there are three major areas where human-computer interaction is important: authentication, security operations, and developing secure systems. A computer operating systems,mobile phones, ATMs machines, etc.

A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving email from servers, accessing files, databases, networks, web sites, and even reading the morning newspaper online. The password is a very good and strong authentication method still used up to now butbecause of the huge advance in the uses of computer in many applications as data transfer, sharing data, login to emails or internet, some drawbacks of conventional password appears like stolen the password, forgetting the password, week password, etc so a big necessity to have a strong authentication way is needed to secure all our application as possible, so a researches come out with advanced password called graphical password where they tried to improve the security andavoid the weakness of conventional password.

Graphical password have been proposed as a possible alternative to textbased, motivated particularly by the fact that humans can remember pictures better than text. Psychological studies have shown that people can remember pictures better than text Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures.

Current authentication methods can be divided into three main areas:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security. Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords.

The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques.A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI).

The picture-based techniques can be divided into two

- recognition based graphical techniques
- recall-based graphical techniques.

Recognition-based techniques

a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage.

Method 1**:**Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique . In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program. The user will be required to identify the preselected images in order to be authenticated.

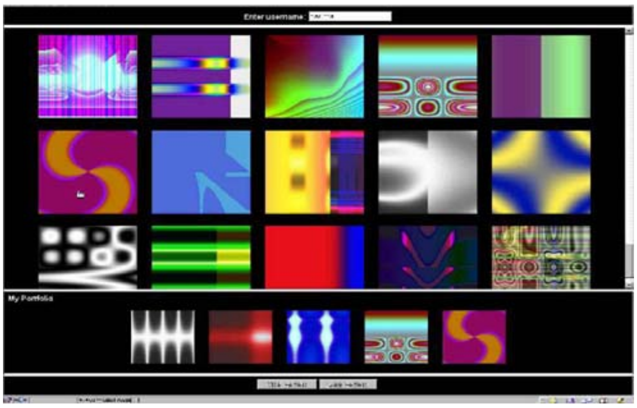


Fig 1: Random images used by Dhamija and Perrig

Method 2**:** Sobrado and Birget developed a graphical password technique that deals with the shoulder surfing problem. In the first scheme, the system will display a number of pass-objects. a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects for authentication.

Method 3: “Pass face” This technique was developed by Real User Corporation. The basic idea is as follows:The user will be asked to choose four images of human faces as their future password. In authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds.

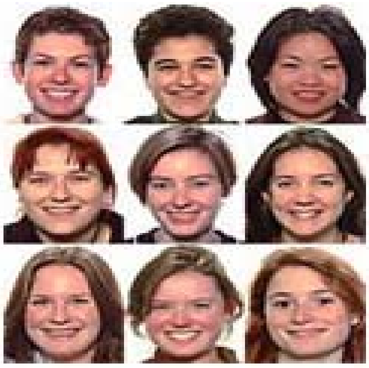


Fig 2:“Pass face” technique

Recall Based Techniques

A user is asked to reproduce something that he or she created or selected earlier during the registration stage.Jermyn proposed a technique, called "Draw-a - secret (DAS)" allows the user to draw their unique password . A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. DAS[Draw-A-Secret] allows the user to draw their unique password . A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated.

Captcha

Captcha relies on the gap of capabilities between humans and bots in solving certain hard AI problems. There are two types of visual Captcha: text Captcha and Image-Recognition Captcha (IRC). The former relies on character recognition while the latter relies on recognition of non-character objects. Security of text Captchas has been extensively studied.The following principle has been established: text Captcha should rely on the difficulty of character segmenta-tion, which is computationally expensive and combinatorially hard .

Machine recognition of non-character objects is far less capable than character recognition. IRCs rely on the difficulty of object identification or classification, possibly combined with the difficulty of object segmentation. Asirra relies on binary object classification: a user is asked to identify all the cats from a panel of 12 images of cats and dogs. Security of IRCs has also been studied. Asirra was found to be susceptible to machine-learning attack. IRCs based on binary object classification or identification of one concrete type of objects are likely insecure . Multi-label classification problems are considered much harder than binary classification problems. Captcha can be circumvented through relay attacks whereby Captcha challenges are relayed to human solvers, whose answers are fed back to the targeted application.

In CaRP, a new image is generated for every login attempt, even for the same user. CaRP uses an alphabet of visual objects (e.g., alphanumerical characters, similar animals) to generate a CaRP image, which is also a Captcha challenge. A major difference between CaRP images and Captcha images is that all the visual objects in the alphabet should appear in a CaRP image to allow a user to input any password but not necessarily in a Captcha image. Many Captcha schemes can be converted to CaRP schemes, as described in the next subsection. CaRP schemes are clicked-based graphical passwords. According to the memory tasks in memorizing and enter-ing a password, CaRP schemes can be classified into two categories: recognition and a new category, recognition-recall, which requires recognizing an image and using the recog-nized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition and cued-recall, and retains both the recognition-based advantage of being easy for human memory and the cued-recall advantage of a large password space. Exemplary CaRP schemes of each type will be presented later.

Like other graphical passwords, we assume that CaRP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS).A CaRP password is a sequence of visual object IDs or clickable-points of visual objects that the user selects.

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 two recognition-based CaRP schemes and a variation next.

ClickText

ClickText is a recognition-based CaRP scheme built on top of text Captcha. Its alphabet comprises characters without any 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.

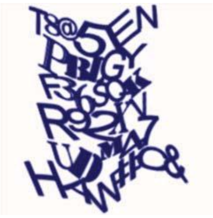


Fig 3: A ClickText image with 33 characters.

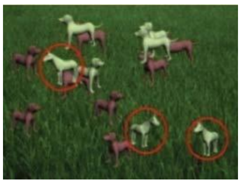
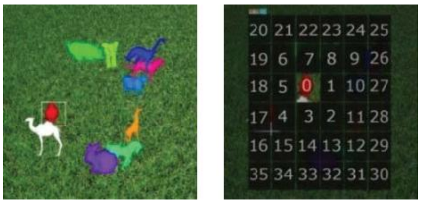


Fig 4: Captcha Zoo with horses circled red.



20	21	22	23	24	25
19	6	7	8	9	26
18	5	0	1	10	27
17	4	3	2	11	28
16	15	14	13	12	29
35	34	33	32	31	30

Fig 5: A ClickAnimal image (left) and 6 × 6 grid (right) determined by red turkey's bounding rectangle.

ClickAnimal

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. 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.

AnimalGrid

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. CaRP should have a sufficiently-large effective password space to resist human guessing attacks.

Recognition Recall CaRP

In recognition-recall CaRP, a password is a sequence of some invariant points of objects. An invariant point of an object (e.g. letter "A") is a point that has a fixed relative position in different incarnations (e.g., fonts) of the object, and thus can be uniquely identified by humans no matter how the object appears in CaRP images.

TextPoints

Characters contain invariant points. A point is said to be an internal point of an object if its distance to the closest boundary of the object exceeds a threshold. A set of internal invariant points of characters is selected to form a set of clickable points for TextPoints. The internality ensures that a clickable point is unlikely occluded by a neighboring character and that its tolerance region unlikely overlaps with any tolerance region of a neighboring character's clickable points on the image generated by the underlying Captcha engine. In determining clickable points, the distance between any pair of clickable points in a character must exceed a threshold so that they are perceptually distinguishable and their tolerance regions do not overlap on CaRP images.

TextPoints4CR

For the CaRP schemes presented up to now, the coordinates of user-clicked points are sent directly to the authentication server during authentication. For more complex protocols, say a challenge-response authentication protocol, a response is sent to the authentication server instead. TextPoints can be modified to fit challenge-response authentication. This variation is called TextPoints for Challenge-Response or TextPoints4CR.

III. Conclusion And Future Works

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords .Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. We have proposed CaRP, a new security primitive relying on unsolved hard AI problems. CaRPis both a Captcha and a graphical password scheme. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks.

A new CaRP image, which is also a Captcha challenge, is used for every login attempt to make trials of an online guessing attack computationally independent of each other. A password of CaRP can be found only probabilistically by automatic online guessing attacks including brute force attacks, a desired security property that other graphical password schemes lack. Hotspots in CaRP images can no longer be exploited to mount automatic online guessing attacks, an inherent vulnerability in many graphical password systems. CaRP forces adversaries to resort to signicantly less efficient and much more costly human-based attacks.

The results of our experiments show that the future research should concentrate on improving the login time and memorability.When a user inputs the corresponding substrings which belong to different CAPTCHAs, the time gap is longer than the time between two characters in one substring. So a method for narrowing the time gap in the entering process and reduction of the impact of users choice trend on security, provide other areas for future research. The CbPA-protocols described require a user to solve a Captcha challenge in addition to inputting a password under certain conditions. For example, the scheme described applies a Captcha challenge when the number of failed login attempts has reached a threshold for an account. A small threshold is applied for failed login attempts from unknown machines but a large threshold is applied for failed attempts from known machines on which a successful login occurred within a given time frame.

References

[1] Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords Learning from the first twelve years", ACM Comput. Surveys, vol. 44, no. 4, 2012.J.

[2] 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 to 15.

[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. 273 to 292, 2008.

[4] 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 to 127, Jul. 2005.

[5] P. Golle, Machine learning attacks against the Asirra CAPTCHA, in Proc. ACM CCS, 2008, pp. 535 to 542.

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

[7] B. B. Zhu *et al.*, "Attacks and design of image recognition CAPTCHAs," in *Proc. ACM CCS*, 2010, pp. 187–200.

[8] J. Yan and A. S. El Ahmad, "A low-cost attack on a microsoft CAPTCHA," in *Proc. ACM CCS*, 2008, pp. 543–554.

[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.