Survey on Captcha as Graphical Passwords

Bhupendra Shivhare
Department of Computer science and Engineering
Oriental Institute of Science and Technology, Bhopal, Madhya Pradesh, India

Jijo S Nair
Department of Computer science and Engineering
Oriental Institute of Science and Technology, Bhopal, Madhya Pradesh, India

Abstract- Text passwords are commonly used in authentication. But text password suffers various attack like dictionary attack, relay attack etc and text password is also difficult to remember. If we make an easy text password then it is easy to crack or if we make a difficult password then it is difficult to remember. The solution of this problem in some context is to make our password in graphical form. A study shows that human can better remember images as compared the texts. Also graphical password provides better security as compared to text password. Combining of graphical password in Captcha technology is commonly known as Captcha as gRaphical Passwords (CaRP). If we use concept of combining of Captcha and graphical password in authentication then it is more beneficial in security perspective such as online guessing attack, relay attack and if combined with dual technologies, shoulder surfing attack. CaRP is well solution of image hotspot problem that is occurs in click-based graphical password. In this paper we have taken a survey on graphical password and CaRP. CaRP concept is based on hard Artificial Intelligence. Hard AI is emerging new concept and it is under explored.

Keywords– Graphical Passwords, Captcha, CaRP, CbPA, Security primitives.

I. INTRODUCTION

CAPTCHA stands for Completely Automated Public Turing Test to tell Computers and Humans Apart [1]. Captcha is used for preventing filling automatic form, automated filling email registration, automated online voting et cetera. These effects reduce network speed and increase unnecessary storage on server. In recent time Captcha and text password used in authentication [2]. Graphical password was invented by Greg E. Blonder in 1995. Various types of graphical password have been developed till now. Security of graphical password is also an open question and various solutions have been made. A fundamental task in security is to make cryptographic primitive based on hard mathematical problems that are intractable. For example, the discrete logarithm problem is main task to the ElGamal encryption, the digital signature, the Diffie-hellman key exchange and so on. By using hard AI problems in security is new field and Captcha is come in this field [3]. This paper will provides you knowledge of CaRP and various types of graphical password schemes. CaRP is a click-based graphical password scheme where a sequence of clicks on image is used to generate a password. CaRP is differs to other click-based graphical password because in CaRP a new image is generated in every login attempt. CaRP is also provides better usability as compared to other graphical password schemes.

II. GRAPHICAL PASSWORDS

Starting around 1999, various types of graphical password scheme have been proposed [4]. Graphical passwords are knowledge based authentication process. We are going to provide schemes that have done by the researchers in this field. There are mainly three types of graphical password

A. Recognition-based

It is also known as cognometric system [5] or searchmetric system [6].In Recognition-based graphical password user to memorize a portfolio of images during password creation. In authentication user then recognize their images from among decoy to log in. Humans have remarkable quality to remember faces [7] [8]. Recognition-based system uses various types of images like random art, faces, natural images et cetera. In this scheme the system must know which image is belongs to user's portfolio.

Passfaces is example of Recognition-based graphical password [9]. In Passfaces user pre- select a set of human faces. During authentication, a panel of candidate faces is presented. User selects the face belonging to their set from among decoys

Figure 1 : Passfaces scheme

Figures 1 illustrate the concept of Passfaces. In other scheme the images of portfolio is ordered and user must require these images in that order while in authentication [10]. Déjà Vu is also similar to this but uses a large set of computer generated 'random art' images [11].

B. Recall-based

A recall-based scheme requires a user to regenerate the same interaction result with no cueing. Draw-A-Secret (DAS) was the first recall-based scheme [12]. In DAS user draw her/his password on a 2D grid. The system encodes the chain of grid cells along a drawing path as a user drawn password. We can get better the DAS's usability by encoding the grid intersection points rather than the grid cells [13].

Figure 2 : Draw-A-Secret scheme

Background images to DAS to encourage users to more difficult password. It is known as BDAS [14].

C. Cued-recall

In cued-recall scheme, an external cue is given to help memorize and enter a password. PassPoins is widely used for this purpose [15].

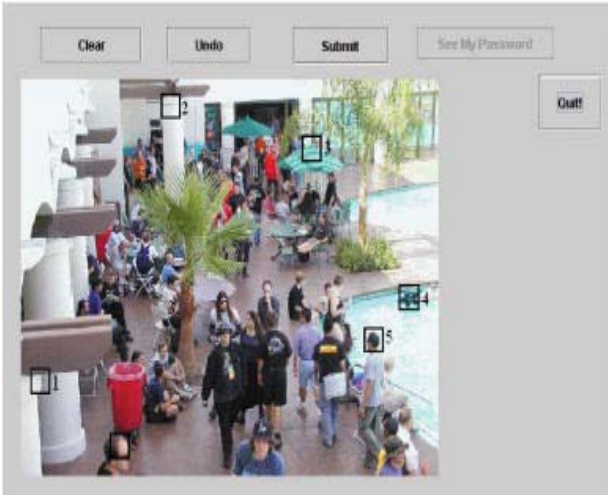

Fig 3 : - PassPoints scheme

It is a clicked-based approach wherein a user clicks a sequence of points anywhere on images in creating a password and re-clicks the same sequence while in authentication. Cued click points [16] is similar to PassPoints but uses one image per click, with the next image is chosen by deterministic function.

Persuasive cued click points [17] extend CCP by selecting points inside a randomly positioned viewport when creating a password. It resulting in more randomly distributed click points in password.

III. CAPTCHA

S Captcha is used to prevent automatic filling the registration form, automatic email creation etc. in a broader way Captcha relies on the gap of capability between humans and bots in solving certain AI problems. There are two types of visual Captcha: text Captcha and Image-Recognition Captcha. The former relies on character recognition while the latter relies on recognition of non-character objects.

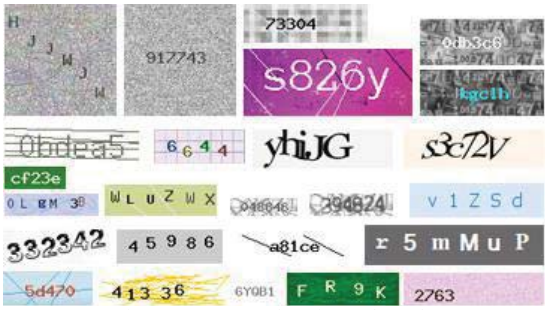

Fig 4 : Some examples of Captcha style

IV. CAPTCHA IN AUTHENTICATION

To counter the dictionary attack it is show [18] that both Captcha and password are used in the user authentication which is known as Captcha based Password Authentication (CbPA) protocol. The CbPA protocol [18] requires a solving a Captcha challenge after inputting a valid pair of user ID and password. The user has the certain probability to solve a Captcha challenge before being denial access. An improved CbPA-protocol is proposed in [19] by storing cookies only on user-trusted machines and apply a Captcha challenge only when the number of failed login attempts for the account has exceeded a threshold. It is further improved by applying a little threshold for failed login attempts from unknown machines but a huge threshold for failed attempts from known machines with a previous successful login in a given time frame [20]. If we use Captcha with recognition-based graphical passwords then it addresses well spyware attack [21] [22].

V. CAPTCHA AS GRAPHICAL PASSWORD

All text Captcha and most of image recognition Captcha can be converted in CaRP. In CaRP, a new image is generated for every login attempt. A major difference between Captcha images and CaRP images is that all the visual objects in the alphabet should come out in a CaRP image to allow a user to input any password but this is not happen in the case of Captcha image.

VI. RECOGNITION-BASED CARP

In this scheme, a password is a chain of visual objects in the alphabet [23]. We present ClickText recognition-based CaRP scheme.

A. ClickText

This is based on text Captcha. ClickText alphabet comprises characters without any visually confusing characters. For example digit ‘O’ and letter ‘0’ may cause confusion so one character should be executed. A ClickText password is a series of characters in the alphabet. ClickText is differs from text Captcha challenge because in this user clicks on characters of the image.

Fig 4: A clickText image with 33 characters

B. ClickAnimal

Captcha Zoo is an image recognition method [24]. It uses 3D models of two similar animals. We can turn Captcha Zoo into a CaRP scheme, by introducing additional akin animals such as pig, horse and dog into the alphabet.

Fig 5: Captcha Zoo with horses circled red

VII. RECOGNITION-RECALL CaRP

In Recognition-recall CaRP, a password is a chain of some invariant points of objects. An invariant point of an object is a point that has a fixed relative place in different incarnations of the object. To enter a password, a user must recognize the objects in a CaRP image, and then use the recognized objects as cues to trace and click the invariant points matching her/his password. Each password point has a tolerance range that a click inside the tolerance range is acceptable as the password point. Nearly all people have a click variation of 3 pixels or less [16]. TextPoint is a recognition-recall CaRP scheme with an alphabet of characters.

VIII. SECURITY PRIMITIVES

A. Security of Captcha

A Captcha challenge typically contains 5 to 8 characters, whereas a CaRP image typically contains more than 30 characters. So it is more difficult to break CaRP image.

B. Automatic Online Guessing Attack

This attack can find a password only probabilistically no issue how many trials are executed. Even if the password guess to be tested in a test is the real password, the test has a minor possibility to succeed since a machine cannot know the objects in the CaRP image to input the password correctly.

C. Human Guessing Attack

In human guessing attacks, humans are used to go through passwords in the trial and error process. Humans are slower than computers in mounting guessing attacks. For 8-character passwords, the password space is $33^8 \approx 2^{40}$ for ClickText with an alphabet of 33 characters, $10^8 \approx 2^{26}$ for ClickAnimal with an alphabet of 10 animals.

D. Relay Attack

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 crack Captcha challenges given little payments. The task to perform and the image used in CaRP are very different from those used to crack a Captcha challenge. This noticeable distinction makes it hard for a human being to mistakenly help test a password guess by attempting to solve a Captcha challenge. Therefore it would be unlikely to obtain a large number of unwitting people to mount human guessing attacks on CaRP. In addition, human input obtained by performing a Captcha job on a CaRP image is useless for testing a password guess.

E. Shoulder-Surfing Attack

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

VII. CONCLUSION

In this paper we have provide a literature on various types of Graphical password schemes and a new security primitive based on unsolved AI problem i.e. Captcha as gRaphical Password (CaRP). Image hotspot problem and guessing attack can thwart by using CaRP. It is also can be used to prevent relay attack and shoulder-surfing (if we combine with dual-view technology). CaRP can also facilitate decrease spam Emails sent from a Web email service. CaRP does not rely on any exact Captcha scheme. When one Captcha scheme is broken, a new and more safe scheme may emerge and be converted to a CaRP scheme.

REFERENCES

[1] L. von Ahn, M. Blum, and J. Langford, "Telling Human and Computers Apart Automatically," in Communications of the ACM, vol. 47, February 2004, no. 2, pp. 57-60. DOI:10.1145/966389.966390.

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

[3]]. 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.

[4] 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.

[5] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63(1-2):128{152, 2005.

[6] K. Renaud. Guidelines for designing graphical authentication mechanism interfaces. International Journal of Information and Computer Security, 3(1):60{85, June 2009.

[7] D. Nelson, V. Reed, and J. Walling. Pictorial Superiority E_ect. Journal of Experimental Psychology: Human Learning and Memory, 2(5):523{528, 1976.

[8] L. Standing, J. Conezio, and R. Haber. Perception and memory for pictures: Single-trial learning of 2500 visual stimuli. Psychonomic Science, 19(2), 1970.

[9] The Science Behind Passfaces [Online]. Available:http://www.realuser.com/published/ScienceBehindPassfaces.pdf

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

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

[12] 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.

[13] 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.

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

[15] 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.

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

[17] 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

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

[19] P. C. van Oorschot and S. Stubblebine, "On countering online dictionary attacks with login histories and humans-in-the-loop," ACM Trans. Inf. Syst. Security, vol. 9, no. 3, pp. 235–258, 2006.

[20] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," IEEE Trans. Dependable Secure Comput., vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.

[21] H. Gao, X. Liu, S.Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in Proc. Symp. Usable Privacy Security, 2009, pp. 760–767.

[22]]. 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.

[23]]. Bin B. Zhu and Jeff Yan "Towards New Security Primitives Based on Hard AI Problems" Security Protocols 2013, LNCS 8263, pp. 3–10, 2013. ©Springer-Verlag Berlin Heidelberg 2013.

[24]]. Lin, R., Huang, S.-Y., Bell, G.B., Lee, Y.-K.: A new Captcha interface design for mobile devices. In: Australasian User Interface Conference (2011).