Asian Journal of Science and Applied Technology (AJSAT)
Vol.3.No.1 2015 pp.66-69
available at: www.goniv.com
Paper Received :08-03-2015
Paper Accepted:20-03-2015
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor : Prof. P.Muthukumar

IMAGE ORIENTED GRAPHICAL PASSWORDS:A NEW PRIMITIVE ENHANCING SECURITY

VIDYAVISWANATHAN[1] , M.ANBARASAN[2]
[2]Assistant Professor,(CSE),.([1]P.G Student,CSE),
Tagore Engineering College, Chennai,India

ABSTRACT

Security is the inevitable requirement of information. Graphical passwords are now much common among the security enhancing methods.Images play a vital role while talking about the graphical passwords.In a broader sense,images are the center point in the graphical password system. Images can be employed in a variety of ways in graphical passwords to enhance the mechanism of security.In this paper,a graphical password system approach which makes use of the image click points is employed. It is supported by sound signature and a captcha enabled graphical password technology called Graphical Captcha System(GCS)is used to ensure the security ofinformation.The proposed is a framework based on AI which involves cognition. GCS also appear to fit with some practical applications for improving online security.

Index terms -Graphical password,Graphical Captchasystem, Security,Captcha, security attacks.

I.INTRODUCTION

A number of password systems exist today.Most of them are based on Mathematical problems,where some others are on the basis of artificial intelligence.Captcha is a technology which makes use of the artificial intelligence. It differentiates human from robots and other spammers. The Captcha enabled technology GCS is accompanied by the graphical password technology.GCS can be developed using two instances.one is based on textual captcha and the other is on the basis of image.Captcha is now facilitated as a standard method of security in the internet services.It is a protective mechanism against online attacks.GCS is employed as a click based graphical scheme in which a series of clicks on different images is used to derive a passwords.The GCS technology provides protection from relay attacks,shoulder surfing attacks and so on.While using GCS,for every login process,a captcha has to be solved by the user.GCS involves different arenas of applications, which include:

1) Usability in touch screen enabled devices.
2) Usability in websites for ticket booking process.

II. BACKGROUND AND RELATED WORK.

A.Graphical Passwords

A graphical password can be stated as a password system which uses images as the main component.The user has to try with these images in a number of ways in different manner to provide security to the particular information as per their requirement. Numerous graphical password technologies exist.They are categorized according to their specific features.Recognition,Recall,Cued recall are the existing categories of graphical passwords.

In the recognition category,the user has to recognize the particular visual and select the suitable one from a given series.The correctness of the image and the order in which they appear in the series are also important for a successful login by the user.An example of this scheme is the passfaces technique where a series of faces appear in place of the images.The user has to identify the appropriate facial image for their profile.

In a recall based approach the user has to reproduce the same result without any failure.The first recall based scheme was known as Draw –a-Secret(DAS).The user draws the password on a 2D grid.This interaction by the user on the grid cells is encoded as the password. The path of drawing the password is also important.Background Draw A Secret(BDAS) is another technology associated with the Draw A Secret scheme,where background images are associated to generate passwords that are hard. In a cued recall based approach, an external cue is supplied to the user.This will help the user to memorize the password they has created. Among the above said three categories the process of recognition is considered as the most easiestone for users whereas recalling process is considered to be the hardest.

B.Captcha

Captcha is Completely Automated Public Turing test to tell Computer and Human Apart.Use of artificial intelligence for security purpose is promoted by means of Captcha technology.Captcha is one which distinguishes human from bots by means of cognitive process. Different varieties of captcha exist,textual captcha, image recognition captcha and audio captcha.In textual captcha text like characters and numerical has to be identified.In image recognition captcha non-characters like images are to be identified.In audio Captchaaudio has to be identified by the user. Captcha find its application in e-mail services such as gmail,yahoo and so on.

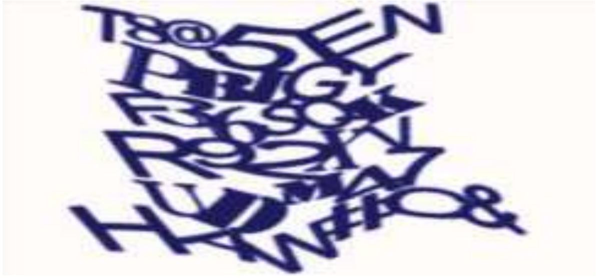


Fig.1.A Click Text image with 33 characters.

C.Captcha in Authentication

Both password and Captcha has been introduced in a user authentication protocol(CbPA) to counter online dictionary attacks.The CbPA protocol requires solving a captcha after a valid user id and password has been given as input. An improved CbPA protocol proposed is such that storing cookies only on user trusted machines and a captcha challenge is applied if a number of login attempt exceeds the threshold.

III.GraphicalCaptcha System

A.GCS: A look up.

In the GCS scheme, a new image is generated for every user login.The GCS image is a Captchachallenge. The user must click on particular points in the images to set the password.GCS schemes are click-based graphical passwords.GCS schemes are of two types, Recognition and recognition recall.

B.Recognition

In this method,a sequence of visual objects in the alphabet is considered as a password.Click text is a recognition based scheme based on textual captcha.Characters are arranged in a random manner in click text images.These are all performed on a 2D grid.Click animal is yet another click-based scheme which makes use of the 3D models.

C.Recognition Recall

In this scheme a series of click points on an image or a textual alphabet is used to derive a password.This is beyond the capability of a bot to find out the password.There are no pre-defined click points.The user itself selects their own clickable points according to their wish and as per the requirement.Hence the password is a sequence of points in images that are clickable.Selecting the click points constitute the recognition.Recall is favored by means of a sound signature along with the click points.

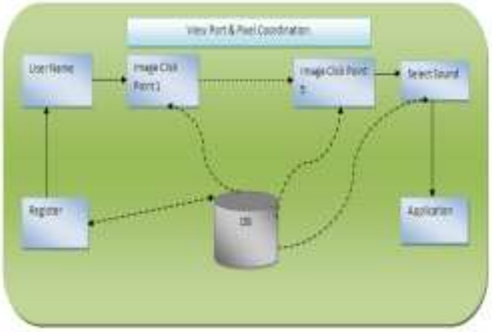
D.Image Generation

An image is uploaded by the user when they are performing the sign up process.After the completion of sign up,the user do the login process. When the user tries to perform the login process later,the uploaded images appear one by one. User has to click on the correct click point of the images in the sequence,that has already set up by the user itself previously.

E.Authentication

While performing the clicking of images,the sign up time click points and login click points must match with each other.If perfect matching occurs,login is succeeded else failure occurs and access is denied.

IV.SYSTEM ARCHITECTURE.



The user performs the registration process initially with the user name and other details.Then they have to choose images according to their requirement and upload it.Then they must set the click point in the image.The activities are supported by the sound signature selected by the user to remember their click point password later.

V.SECURITY ANALYSIS.

A.Security of underlying Captcha

As a framework of graphical passwords,GCS doesn't relay on any particular captcha. Actually it is not captcha but a technology similar with captcha. If one Captcha scheme gets broken a new and more robust Captcha scheme may appear to construct a new GCS scheme.

B.Automatic Online guessing attacks.

In this type of attacks,the trial and error process is executed automatically whereas dictionaries can be constructed manually.

C.Human Guessing attack

In human guessing attacks,humans are used to enter the passwords in trial and error process.Compared to computers, human are much slower in mounting guessing attacks.Usually the users tend to use a textual password of 6-8 characters.It is guessable by others,where clickable passwords have least probability of guessing than textual passwords.

D.Shoulder Surfing attacks

Shoulder surfing attacks are a threat when graphical passwords are entered in a public place such as bank ATM machines. GCS is not robust to shoulder-surfing attacks.

VI.CONCLUSION

The proposed is a new security primitive based on AI problems.It is on the basis of cognition process.GCS is both a captcha and a graphical password.The new approach is a counter measure to online guessing attacks.A new image and a required click point can be used by the user for every login attempt. This makes the trials of an online guessing attack computationally independent of each other. Even though the proposed framework is on the basis of captcha technology,GCS doent relay on any specific captcha.Overall this work is another step forward in using the paradigm of AI for security.

REFERENCES

[1] 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.

[2] (2012, Feb.). The Science BehindPassfaces[Online]. Available:
http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[3] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The designand analysis of graphical passwords," in Proc. 8th USENIX SecuritySymp., 1999, pp. 1–15.

[4] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability ofgraphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292,2008.

[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon,"PassPoints: Design and longitudinal evaluation of a graphical passwordsystem," Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.

[6] P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawngraphical passwords," ACM Trans. Inf. Syst. Security, vol. 10,no. 4, pp. 1–33, 2008.

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

[8] A. E. Dirik, N. Memon, and J.-C.Birget, "Modeling user choice in thepasspoints graphical password scheme," in Proc. Symp. Usable PrivacySecurity, 2007, pp. 20–28.

[9] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting
hot spots in graphical passwords," in Proc. USENIX Security, 2007,pp. 103–118.

[10] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated
attacks on passpoints-style graphical passwords," IEEE Trans. Inf.Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010.

[11] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in clickbased
graphical passwords," J. Comput. Security, vol. 19, no. 4,pp. 669–702, 2011.

[12] T. Wolverton. (2002, Mar. 26). Hackers Attack eBay Accounts[Online]. Available:
http://www.zdnet.co.uk/news/networking/2002/03/26/hackers-attack-ebay-accounts-2107350/

[13] HP Tipping PointDVLabs, Vienna, Austria. (2010). Top Cyber Security
Risks Report, SANS Institute and Qualys Research Labs [Online].
Available: http://dvlabs.tippingpoint.com/toprisks2010

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

[15] 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.

[16] 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.

*[17] 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.*

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