International Journal of Communication Networks and Security

Volume 1 | Issue 4 Article 9

April 2012

A NEW APPROACH FOR INSTIGATING SECURITY USING SINGLE ZOOM MOUSE CLICK GRAPHICAL PASSWORD

MERIN SEBASTIAN
Rajagiri School of Engineering and Technology, Rajagiri Valley, Kakkanad, Kochi , Kerala, India,
merinsebastian59@gmail.com

BIJU ABRAHAM NARAYAMPARAMBIL
Rajagiri School of Engineering and Technology, Rajagiri Valley, Kakkanad, Kochi , Kerala, India,
bijuan@rajagiritech.ac.in

A NEW APPROACH FOR INSTIGATING SECURITY USING SINGLE ZOOM MOUSE CLICK GRAPHICAL PASSWORD

MERIN SEBASTIAN[1] & BIJU ABRAHAM NARAYAMPARAMBIL[2]

[1,2]Rajagiri School of Engineering and Technology, Rajagiri Valley, Kakkanad, Kochi , Kerala, India
E-mail: merinsebastian59@gmail.com & bijuan@rajagiritech.ac.in

Abstract – Due to growing hazards to networked computer system, there is great need for security innovations. Authentication is the process of security to information. User authentication is one of the significant topics in information security. Commonly used authentication is alphanumeric passwords, biometrics and smart card. At present day upcoming popular method is graphical password. In graphical password systems authentication is based on clicking on image rather than typing alphanumeric strings .The motivation to develop graphical password is the fact that human can remember picture better than text. In this we propose a graphical password scheme which is more secured than other method. This method also depends not only on image but also number of mouse click on the image. This method reduces the huge image database, as well as images being too simple to cause collisions on points selected for different users.

Keyword: *Graphical password, Alphabetic dictionary, cued recall.*

I. INTRODUCTION

Graphical passwords are an alternative authentication method to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings. The user input the password to the computer in graphical password with an aid of the computers graphical input devices and output devices. The user select from images, in a specific order, presented in a graphical user interface (GUI)[3]. For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA). The graphical-password approach increases the usability feature and memory of the user. Graphical password tries to overcome major drawback of alphanumeric passwords. The alphanumeric passwords has the drawback as password is easy to guess, user has to remember the password always, cracking the password was easy, complex password has to be created for security , different password has to maintain for different authentication.

Though graphical password has been implemented widely there still few drawbacks :(1) The password might be easily guessed when there exits too few picture; (2) Many passwords might be identical if the pictures are homogeneous; (3) similar to text passwords, the adversaries can view the user's input process by shoulder surfing, and try to impersonate the user later on;

In this paper, proposed scheme will reduce this drawback .Proposed scheme also depends on number of click and alphabetic dictionary scheme on the image so there can be single image or collection of image. Shoulder attack is almost unfeasible in this method.

The paper is organized as follows: Section 2 we brief of present graphical password schemes. Section 3 describes the proposed scheme and the working of alphabetic dictionary scheme will. Section 4 and 5 future work and conclusion will be discussed.

II. OVERVIEW OF GRAPHICAL PASSWORD SCHEME

In normal authentication method the user has to give the user name and the alphanumeric password. Graphical password works same as alphanumeric password the user has to enter the name and the password, but the password will be images [2][3]. The user has to click on the image in sequences. The sequences of click will become the password. By using the images the user can easily identify password. The steps involved during authentication are

Step 1: On logging in the user has to give his/her user name.
Step 2: The user has to click on the particular image which he/she selected as password during registration .
Step 3: The sequences of the click has to be the same as the user click during registration.
Step 4: The sequences of click is noted and checked with the data base.
Step 5: The user is authenticated, if the correct sequences is given.
Step 6: If not authenticated the user has to go thought the authentication process again.

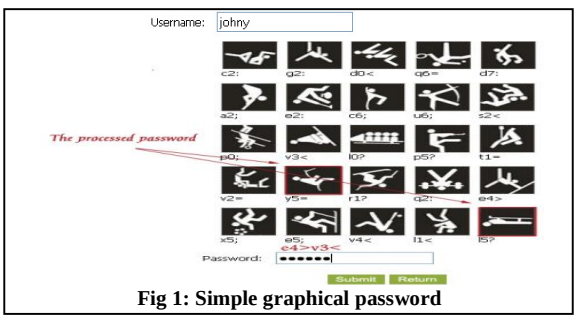

Fig 1: Simple graphical password

The graphical password scheme has been divide into three [1] 1) Recall (Something you know) 2) recognition (Something you recognize) 3) CCP(Cued-recall).

A. Recall method

Recall base techniques is something which the user know. A secret is shared between the user and the system. Users must recall and correctly enter their secret to authenticate themselves. Anyone who knows or guesses the secret will also be able to authenticate as the original user. Several method developed are,

a) **Draw-A-Secret (DAS):** Users draw their password on a 2D grid using mouse[1][3] .The password is composed of the coordinates of the grid cells that the user passes through while drawing. A drawing can consist of one continuous pen stroke or several strokes.

b) **Blonder Algorithm:** This graphical password scheme in which a password is created by having the user click on several locations on an image[1][7]. During authentication, the user must click on the approximate areas of those locations.

c) **Pass-Go:** User draw their password on a grid, except that the intersections are used instead of grid squares. Visually, the user's movements are snapped to grid-lines and intersections so that the drawing is not impacted by small variations in the trace[1].

d) **Passdoodle**: Passdoodle is similar to DAS, allowing users to create a freehand drawing as a password, but without a visible grid. The use of additional characteristics such as pen colour, number of pen strokes, and drawing speed are suggested by the authors to add variability to the doodles[1].

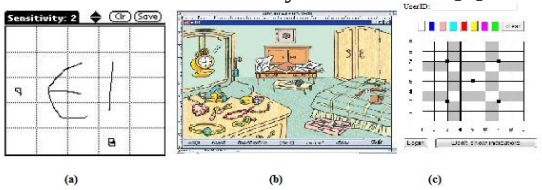

Figure 2: (a) DAS (b) Blonder algorithm (c) Pass Go

B. Recognition

Recognition techniques are something which user recognize. The user and the system share a secret. The system provides cues and the user must correctly recognize the secret. Anyone able to recognize the secret will be able to authenticate as the original user. Graphical passwords where users must recognize pre-selected images from a set of decoys fall into this category. Several method developed are,

a) **Dhamija and Perrig Algorithm**: user will be asked to select certain number of images from a set of random pictures generated by a program. Later, user will be required to identify the pre-selected images to be authenticated[1][8].

b) **Sobrado and Birget Algorithm**: This technique that overcome the shoulder surfing attacks[1][7]. In their first scheme which they called "triangle scheme", a user needs to selects their pass-object among many displayed object. To be authenticated,a user needs to recognize all the pre-selected pass-object which was selected during the registration phase. The user requires to click inside the convex-hull which formed by the pass-object.

c) **Man Algorithm**: a user selects a number of pictures as pass-objects. Each passobject has several variants and each variant is assigned a unique code[1]. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects.

d) **Jansen Algorithm**: For the password creation, a user has to select the theme first which consists of thumbnail photos[7][8]. Afterward, a user has to selects and registers a sequence of the selected thumbnail photo to form a password.

e) **Passface Algorithm**: Based on the assumption that human can recall human faces easier than other pictures [1]. User are requires to select the previously seen human face picture from a grid of nine faces which one of the face is the known face and the rest is the decoy faces.

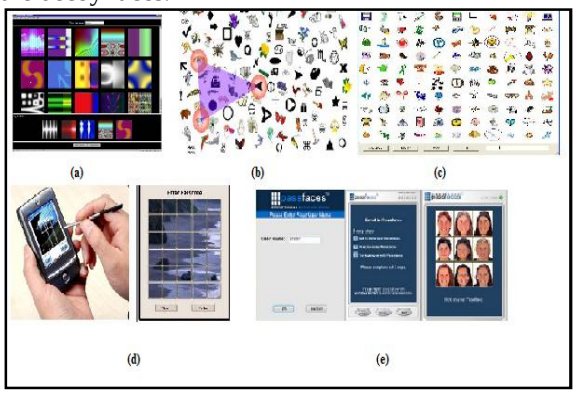

Figure 3: (a) Dhamija and Perrig (b) Sobrado and Birget (c) Man Algorithm (d) Jansen (e) Passface

C. Cued Recall

Cued-recall is combination of recall and recognition scheme. Thus it is more secured than other methods. In cued-recall systems, the system provides a cue to help trigger the user's memory of the password. This feature is intended to reduce the memory load on users and is an easier memory recall task than pure recall. Several method developed are,

a) **Cued Click Points (CCP):**It is combination of PassPoints, Passfaces. A password consists of one click-point per image for a sequence of images[6]. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. (see fig 4 (a))CCP offers both improved usability and security Users had high success rates, could quickly create and re-enter their passwords, and were very accurate when entering their click-points.

b) **Click Button According to Figures in Grid(CBAFG):**

This is improvement made to CCP scheme. In this multiple background images is adopted. On registration user is presented with four background image[5]. User should choose one or more image from four background image. The "n" pass-image is displayed in turn for the user to select several cells as password by clicking the image. After selection user choose an icon from ten icon display as staring icon. During authentication there will be 4 background image, 1 icon and 10 numeric button(fig 4(b)). If the icon is not user staring icon then user has to click any numeric button randomly and icon will change on each click. When staring icon appears user can enter password by clicking each cell.

c) **Implicit Password Authentication (IPA):**This is applied in mobile banking. The bank database will have 100 to 200 standard questions[4]. On registrations the user has to pick 10-20 questions from database and provide answer to the selected question. For each question server create an intelligent authentication space using image. The answer to the question will be embedded into image. On authentication, the server picks one or more questions selected by user on registration time randomly .the user need to navigate the image and click the right answer. For example in fig 4(c) first glob is shown. The question is which city user love to visit and the answer is Sydney then user has to click on Australia, and then Australia will enlarge, and then click on Sydney so on.

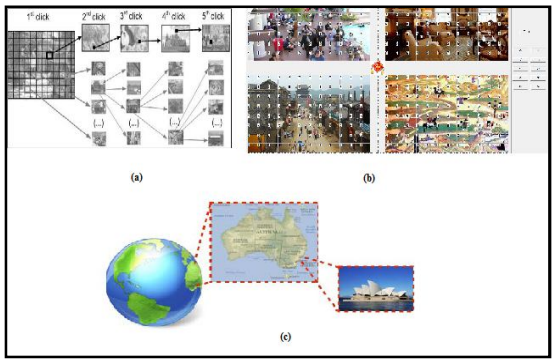

Figure 4: (a)CCP (b) CBAFG (c) IPA

III. OUR SCHEME

In cued recall method there are sequences of image enlargement by clicking on image(fig 4(a)) .It mean that there are "n" image(n- password length)for each user . Thus lot of memory is needed to store the image. Though cued recall is best secured scheme the memory is a problem. The proposed scheme borrow some features of cued recall scheme, Dhamija and Perrig scheme (recall method) and alphabetic dictionary scheme. Our scheme will give better security and usability to the user. Alphabetic dictionary scheme is user to add more security to the system.

In proposed system there is only one level of image enlargement. The user as to click "n" times (n-number of mouse click) on starting image, based on the click point next image is enlarging. The next image is the theme image. The user has to click the particular image and apply alphabetic dictionary (fig 5).

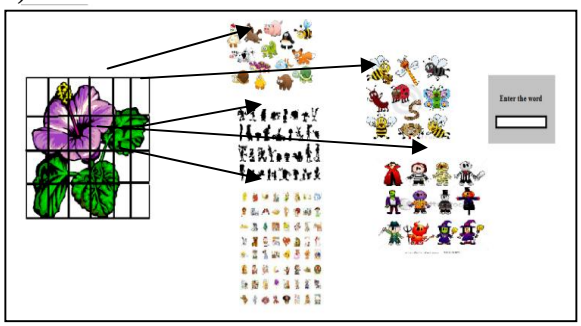

Figure 5: Single zoom mouse click graphical password

Alphabetic dictionary add security to authentication. In this the user has to assign an alphabet to each image in theme image (enlarged image). For that selected alphabet the use has to maintain a set of word starting with the alphabet (special character are included). Each time user log in the user has to click on staring image "n" times(fig 5), then the theme image will come on that click on particular image and type the word.

A. LEVEL OF CHECKING

First checking: User has to click on specific region of the theme image "n" times. For example if the user has kept the number click six, while logging in the user has to continuously click six times on specific region. If the user clicks less than six or more than six the user is unauthenticated. This is done at level 1.

Second checking: According to click in the specific region next theme image is zoomed(like in cued click point). Each grid in the zoomed in image is assigned an alphabet. This is done at level 2. This level uses the alphabetic dictionary scheme and Dhamija and Perrig scheme. The user has to click six specific region (grid) in the theme image and the spell the string with the alphabet assign to that specific region. Each time the user log in the images are rotated according to the Dhamija and Perrig scheme. The rotation is done so the attacker find difficulty in finding the user clicks.

Third checking: In this alphabetic dictionary scheme is advanced by creating a dictionary of alphabet. This dictionary will store a set of string for the alphabet. If the user password length is six, there will be six dictionaries for six alphabets. The user has to spell the string in dictionary when he clicks the image. The string spelled will depend on the number of time the user has log in. If the user is log in for first time, the user has to spell the word which is first in the dictionaries. This will go in round robin method.

IV. FUTURE WORKS

Graphical password is an emerging technology in this world for authentication. There can be more idea developed in this technology and more improvement applied to current development. The technology can also be extended to network security.

V. CONCLUSION

In this paper we have discussed about the graphical password and its different schemes. A small idea of different scheme has been discussed. In proposed scheme a new idea has been implemented. The proposed scheme gives more usability and security to authentication system. There can still more development in this area.

REFERENCE

[1] R. Dhamija and A. Perrig, "D´ej`a Vu:A User StudyUsing Images for Authentication", in Proceedings of the 9th USENIX Security Symposium, 2000.

[2] G. S Owen, X. Suo, and Y. Zhu, "Graphical passwords: a survey", in Computer Security Applications Conference, 21st Annual, 5-9 Dec. 2005 Page(s):10 pp.

[3] J. C. Birget, A. Brodskiy, and N. Memon, S. Wiedenbeck,and J. Waters, "Authentication using graphical passwords:Basic results", in Human-Computer Interaction International (HCII 2005). Las Vegas, NV, 2005.

[4] Sadiq Almuairfi and Parakash Veeraraghavan," IPAS:Implicit Password Authentication System",in Workshops of International Conference on Advanced Information Networking and Applications .Singapore ,2011.

[5] Jinhua Qiu, Xiyang Liu, Licheng Ma,Haichang Gao and Zhongjie Ren ," A Novel Cued-recall Graphical Password Scheme", proceeding 6th International Conference on Image and Graphics Page 949-956, Washington, 2011.

[6] Sonia Chiasson , P. C. Van Oorschot and Robert Biddle," Graphical Password Authentication Using Cued Click-points ", 12th European Symposium On Research In Computer Security (ESORICS), 2007.

[7] Ian JermynAlain Mayer, Fabian Monrose and Michael K. ReiterAviel**,"** The Design and Analysis of Graphical Passwords**",** Proceedings of the 8th USENIX Security Symposium, Washington, 1999.

[8] Haichang Gao, Xiyang Liu, Sidong Wang, Honggang Liu and Ruyi Dai," Design and Analysis of a Graphical Password Scheme "4th International Conference on Innovative Computing Information and Control ICICIC, 2009.

[9] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," 3rd Australasian Conference on Information Security andPrivacy (ACISP): Springer-Verlag Lect. Notes in Computer Science (1438), 1998.

[10] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N.Memon, "Authentication using graphical passwords: Basic results," Human-Computer Interaction International (HCII 2005). Las Vegas, NV, 2005.