Login History and CaRP for User Authentication

Reshma J Chavan
ME Computer Student
Department of Computer Engineering
JSCOE PUNE
Pune, India
chavan2reshma@gmail.com

Prof. M. D. Ingle.
Assistant Professor
Department of Computer Engineering
JSCOE PUNE
Pune, India
ingale.madhav@gmail.com

Abstract: - Password is main vulnerability in computer security. Passwords are commonly guessed by machine programs running dictionary attacks. Passwords main used for the authentication method in spite of security weaknesses. User authentication obviously practical issue. According to the view of a service provider this problem needs to be resolved within real-world constraints such as the available hardware and software infrastructures. According to user's view user friendliness is a basic requirement Click based graphical password scheme provides a different approach to address the familiar image hotspot problem. Graphical password systems such as PassPoints, that frequently leads to weak password choices. So to provide user friend-liness and also the protection from various security attacks. In this, graphical password scheme, the click event is performed on various points on same or different images.

Keywords: *Graphical passwords, password guessing attacks, security primitive, login history.*

*****

I. INTRODUCTION

The security and usability drawback in text based password schemes overcome in the development of graphical password schemes .For this tentative of graphical password schemes have been nominated, provocation by the promise of improved password memorability.In usability, the same time improving strength against guessing attacks. Graphical passwords are knowledge based authentication mechanisms where users enter a shared secret as evidence of their identity. In text passwords involve alphanumeric, special keyboard characters, main concept for graphical passwords is to leverage human memory for visual information of shared secret and composed of images or sketches..

A graphical password can be have nominated in large scale . They can be classified into three categories to the task involved in memorizing and entering passwords: recognition, recall, and cued recall. Each category is explain here. .others can be available in recent review of graphical password.

The main determination for graphical passwords is the hypothesis that people are better at remembering images than artificial words. Visual objects used as a passwords. From thousand of faces user can recognized the faces for authentication system.

Graphical password scheme developed for controlling disadvantages of text based password. Graphical images easily can be process by human brains.In graphical password scheme such as icons ,human faces,custom image to build a password.Due to human characteristics graphical password scheme is better.For preventing dictionary attack graphical password has maximum resistance Many graphical password schemes are already introduced. There are two categories of Graphical password techniques recognition-based and recall based. Series of images are given for authentication correct sequence of images is to given in right order for recognition-based systems, .User asked to create or selected earlier during the registration for recall based .Use of graphical password is increased than text password from past decade

The paper include graphical password as user authentication system. If attacks on graphical password system we introduced new technique login history, user can entered into the system by providing correct login history file.

II. BACKGROUND AND RELATED WORK

Graphical password is easy to recall so need for that is increased.,potential to provide a more symbols space than text based password. For graphical password maximum research is going some of them introduced some ideas and others are still working on them for more secure password. Blonder in 1996 given the idea for graphical password scheme. In these scheme in front of user an image is displayed which is predetermined image on any visual display device which user is using then user has to select one or more positions on image which are already known positions to user in a particular order to access the particular resource[5]. The drawback of these method is user can on known positions only so may be similar as text password. Another A PassPoint[6] method to overcome drawbacks of Blonder's methodIn passpoint [6] predefined boundaries of images are eliminated and arbitrary images are allowed to be used, so that user clicks on an place on image for creating a password. After the password is created a tolerance around each chosen pixel is calculated, then for authentication of user, The user choose the correct sequence within the tolerance when user wants to access restricted resource or any application which is restricted.

In Cued Click Points (CCP), a cued-recall graphical password technique [7], in this technique, a password is composed of one click-point per image for a sequence of 5 images. 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. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. The advantage of CCP over PassPoints is the fact that authorized users get feedback about an error when trying to log in within a second. When users see an incorrect image, they know that the latest click-point was incorrect and can immediately cancel current attempt and the process is started again from beginning.

Grid based schemes are also proposed which uses recall method. In " Draw A Secret" technique , user draw a password on 2D grid .The coordinates of this drawing on the grid are stored in order. For user must redraw the picture for authentication. A user redraw picture during authentication..if user draw correct order on grid then user is authenticated. The diagonals lines are difficult to draw in DAS,and problem might occur when the user chooses a drawing that contains strokes that pass too close to a grid-line .User must pass the input in sufficient way top form the grid lines and intersection for getting correct password. The scheme may not be distinguish if user draw password close to grid lines or intersection. A system where authentication is conducted by having the user drawing his/her signature using a mouse [9].

The advantage of these is to no need to remember the signature and difficult to copy .So everyone is not familiar using the mouse, it is difficult to draw. A graphical authentication scheme [10] during registration user have to select certain number of images from set of random pictures. for authentication user has to identify pre-selected images. The user has given a set of pictures on interface ,some taken from portfolio ,from that user have to select random pictures. User has to select pictures from given characters for authentication.

Passface is a technique developed by Real User Corporation based on the assumption that people can recall human faces easier than other pictures [11]. User is asked to choose four images of human faces from a face database as their password. For traditional authentication in these technique is fill the blank gaps for increasing security level and error tolerance.But unfortunately there is a common weakness in the above graphical password schemes: They are all vulnerable to shoulder-surfing attacks. To address this issue, a graphical password technique [12]. In their scheme, the system first displays a number of 3 pass-objects (pre-selected by a user) among

many kind of images, Many other objects. A user needs to recognize pass-objects and click inside the triangle formed by the 3 pass-objects for authentication.

A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS) [13]. In this scheme, user is provided with the login-image which consists of 93 printable characters. To login, the user must find all his/her original pass-characters in that image and then make some clicks inside the invisible triangles which are called pass-triangles.The pass-triangles are created by 3 original pass-characters following a certain click-rule. In this scheme, user pass-character lies inside the pass-triangle. If the user password length is k then he has to click k-times inside the invisible pass-triangles. In S3PAS if the size of every pass triangle area is too large, attackers are able to click inside the right areas with higher probabilities.

A recognition-based graphical password scheme Color-login[14], An interesting game way to weaken the boring feelings of the graphical authentication is introduced. Uses background color in Color-login,but these a method not previously considered, for reducing login time greatly.The peepers get confused so that variety colors are used , while not burdening the legitimate users. The scheme is resistant to shoulder surfing attack but password space is smaller than text-based passwords. Another shoulder-surfing resistant algorithm in which a user selects a number of pictures as pass-objects[15]. Each pass-object has several variants and a unique code is assigned each variant . the user is challenged with several scenes during authentication. Several pass-objects and many decoy objects contains in each scene . The user has to type in a string with the unique codes for to the pass-object. So these methods force the user to memorize too many text strings, and their shoulder-surfing resistant property is not strong either. In real scenario, these approaches are under-utilized as the authentications are usually complex and boring for users.

ClickAnimal[1] is one more method based on recognition based scheme . So this is captach scheme,

used to generate 2D animals with different textures poses, colors and arranges them on background such as grassland by using 3D models of horse and dog . some animals may be overlapped with each other when the animals are arranged on background ,but main parts are not overlapped in order to recognised by human. A smaller password space for The ClickAnimal than ClickText[1], in ClickText the alphabets are displayed but alphabets are not overlapped user can easily clicks on them to generate or choose the password. Here when user click on any alphabet then location is tracked to check whether user clicks on correct character. ClickText[1] is also the recognition based scheme to generate graphical passwords

III. EXISTING SYSTEM

In existing system [1], CaRP (Captch as gRaphical Password) is used to authenticate the system. Here, Instead of text based password the graphical password is used to authenticate the user. When user requesting for login enters into the system then ,user enter the userID after that the image genetrated, perform click events by the user, if the click events matches with the system database then user authentication is successful otherwise authentication fail. Following figure illustrates the above procedure:

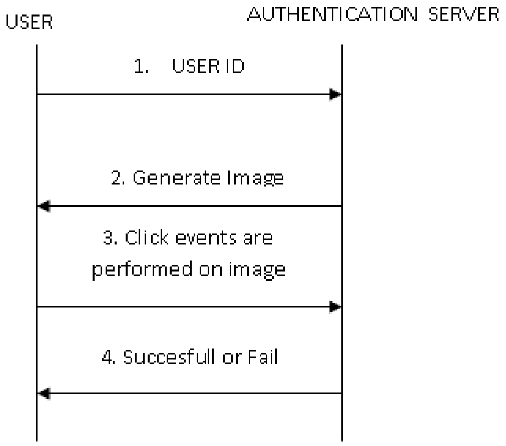

Fig.1 Flow chart of CaRP process.

But the problem with this method is that any person can concentrate and get the password when user is clicking on the image. So new method is introduced to overcome this problem, that method is discussed in section IV.

IV. PROPOSED WORK

In this proposed system we use same CaRP scheme to authenticate the user. But to provide more secure approach login history is initiated. Proposed system contains the following models:

A] Login Histroy:

Login history attributes will select after the registration process, attributes will select like date time.

In second phase attribute will encrypt and will use for next login. During login user will decrypt the file and user will login. Here we can use SHA algorithm for encryption of login history file.

The system architecture is shown in fig.2;

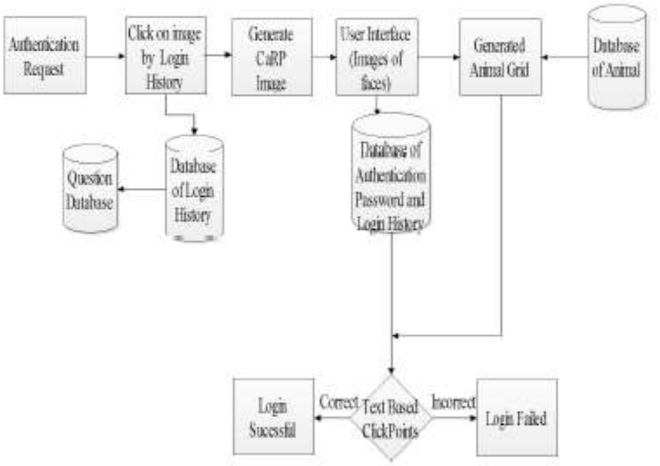

Fig.2 System architecture of proposed system.

V. CONCLUSION

Graphical password scheme will develop for Authentication system, which is based on click based graphical authentication scheme.This will allow to store the database of user and it will be in the form of image click by user for authentication process system. User will click on different points on same image or different image. Click based graphical password scheme provides protection offers protection against relay on passwords and online dictionary attacks, which have been for long time a major security threat for various online services. A proposed method is introduced login history to provide more secure approach to authenticate an user.

ACKNOWLEDGMENT

I like to acknowledge my vigorous thanks to Prof. M.D.Ingale for providing giving suggestions which helped me a lot in my research work and I also want to thanks our friends and classmates for helping me in this research work by giving me there timely suggestions and feedbacks on my research work.

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 Forensics And Security, Vol. 9, No. 6, June 2014.

[2] X. Suo, Y. Zhu, and G. S. Owen, “Graphical passwords: A survey”, 21st Annual Computer Security Applications Conference (ASCSAC 2005).Tucson, 2005.

[3] Md. Asraful Haque, Babbar Imam, Nesar Ahmad, “2- ound Hybrid Password Scheme”, International Journal of Computer Engineering and Technology (IJCET), Vol. 3, Issue 2, July-September (2012), page. 579-587.

[4] D.Weinshall and S. Kirkpatrick, “Passwords You’ll Never Forget, but Can’t Recall”, in Proceedings of Conference on uman Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399- 1402.

[5] G. E. Blonder, “Graphical passwords”, in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent-5559961, Ed. United States, 1996.

[6] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon, “Passpoints: design and longitudinal evaluation of a graphical password system”, International Journal of Human-Computer Studies, 63:102–127, July 2005.

[7] 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, pp. 359-374

[8] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, “The design and analysis of graphical passwords”, Proceedings of the 8th USENIX Security Symposium Washington, D.C., USA, August 23–26, 1999

[9] A. F. Syukri, E. Okamoto, and M. Mambo, “A User Identification System Using Signature Written with Mouse”, in Third Australasian Conference on Information Security and Privacy (ACISP): Springer- Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[10] R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9th USENIX Security Symposium, 2000.

[11] Real User Corporation, “How the Passface System Works”, 2005.

[12] L. Sobrado and J.-C. Birget, “Graphical Passwords”, The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[13] Huanyu Zhao and Xiaolin Li, “S3PAS: A Scalable houlder-Surfing Resistant Textual-Graphical Password Authentication Scheme”, 21st International Conference on Advanced Information Networking and Applications Workshops, AINAW '07. Page(s): 467 – 472.

[14] Haichang Gao, Xiyang Liu, Ruyi Dai, “Design and Analysis of a Graphical Password Scheme”, International Conference on Innovative Computing, Information and Control (ICICIC), 2009, pp. 675 – 678.

[15] S.Man, D. Hong, and M. Mathews, “A Shouldersurfing Resistant Graphical Password Scheme”, In Proceedings of International Conference on Security and Management, Las Vegas, NV, 2003.