ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Paper on authentication of an system using hidden codes and random code generator

Ms. Dhanshri Agashe[1], Prof. A.R Raipurkar[2]

M. Tech Scholar, CSE Department, S.R.C.O.E.M, Nagpur, India[1]

Assistant Professor, CSE Department, S.R.C.O.E.M, Nagpur, India[2]

Abstract: This paper presents an evaluation of image based authentication using hidden codes and random code generated in graphical password scheme. Now a days authentication is a very critical problem in security system. Unauthorized user or hacker can easily stole the information contains in a system by using proxy password or by capturing the gallery where different passwords get generated in it. This has been solved by the fact the humans have a natural inclination to remember images more easily than text. As images are better to remember. Here we have proposed a graphical password authentication where it will consists of number of images and each image is hidden by a specified character which cannot view to user and this will set it as his password for login page. A new algorithm that using watermarking for the images which will be watermarked and Image based authentication using hidden codes and random code generator technique as the solution to solving image gallery attacks and using the random character set generation for each image for resistance to shoulder surfing attack to provide better system secure.

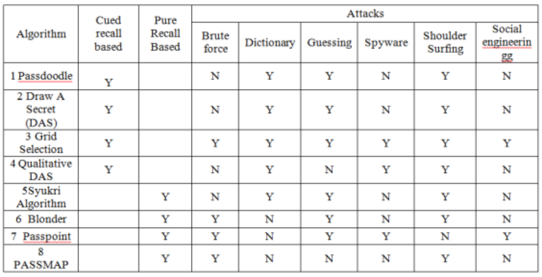
Keywords: Graphical Password, Watermarked Algorithm, Authentication Security, Shoulder surfing ,image gallery attack

I. INTRODUCTION

Human factors are always considered the weakest link in a security of an computer system.[1] Patrick, et al. find out that there are three major areas where human computer interaction is important authentication of data, security , and developing secure systems. It will focus on the authentication problem. Most common computer authentication method is for a user to submit a user name and a text password. Most of the problems is the difficulty of remembering a text passwords. Studies have shown that users has pick a short passwords or passwords that are easy to remember. Unfortunately, these passwords get easily guessed or broken. Graphical password schemes has been proposed as a possible alternative to text-based passwords, by the fact that humans can remember pictures better than text. Pictures are generally easier to be remembered than text. If number of possible pictures is sufficiently large and spacious, the possible password space of a graphical password scheme may exceed that of text based schemes and thus offer better resistance to dictionary attacks. There is having a growing interest in graphical password and it an advantage to this scheme. In addition to workstation and web log-in applications, graphical passwords can also been applied to ATM machines and mobile devices. Here user has selects number of images as a password and while login user needs to enter the random code generated below each image, which has been set as a password. Graphical Password Schemes provide a way of making more human-friendly. Passwords and more secure passwords. The security of the system is very high and every time user have to enter different set of code for authentication i.e. every time new password gets generated. Dictionary attacks, Brute Force attack, image gallery attack ,shoulder surfing attack and other attacks are infeasible on this password scheme.

II. AUTHENTICATION

Authentication is the process of determining the fact that whether someone or something is, who or what it is declared to be. Now a days private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. It will be known that the password is assumed to guarantee that the user is authentic. Everytime user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use when he logon the page, the user must know and use the previously declared password. The main weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen, guessed, accidentally revealed, or forgotten.



Algorithm	Cued recall based	Pure Recall Based	Attacks					
			Brute force	Dictionary	Guessing	Spyware	Shoulder Surfing	Social engineeringg
1 Passdoodle	Y		N	Y	Y	N	Y	N
2 Draw A Secret (DAS)	Y		N	Y	Y	N	Y	N
3 Grid Selection	Y		Y	Y	Y	Y	Y	Y
4 Qualitative DAS	Y		N	Y	N	Y	Y	N
5Syukri Algorithm		Y	N	Y	Y	N	Y	N
6 Blonder		Y	Y	N	Y	N	Y	N
7 Passpoint		Y	Y	N	Y	Y	N	Y
8 PASSMAP		Y	Y	N	N	N	Y	N

Fig1: Different attacks on graphical password

For this reason, Internet business and many other transactions require a more stringent authentication

DOI 10.17148/IJARCCE.2015.43138

process. The use of a digital certificates issued and verified by a Certificate Authority (CA) as part of a public key infrastructure is considered likely to become the standard way to perform authentication on the internet and make secure to the system.

III. RELATED WORK

Dhamija and Perrig [1] proposed a graphical authentication scheme where the user have to identify the pre-defined images to prove user's authenticity. The user in this system selects a certain number of images from a set of random pictures during registration. Later, during login the user has to identify the selected images that he has selected previously for authentication from a set of images. This system is vulnerable to shoulder-surfing attack.

Passface [2] is a technique where the user sees a grid of nine faces and selects one face previously chosen by the user. Here, the user have to chooses four images of human faces as their password and the users have to select their pass image from eight other decoy images which are in a grid. Since there are four user selected images it is done for four times.

Jermyn [3], proposed a new technique called "Draw- a-Secret" (DAS) where the user is required to re-draw the pre-defined picture on a 2D grid that he have to select. If the drawing touches the same grids in the same sequence, then the user is authenticated. This authentication scheme also proves vulnerable to shoulder surfing.

Haichang's [4] proposed a new shoulder-surfing resistant scheme where the user is required to draw a curve across their password images which are been there and orderly than clicking on them directly. This graphical scheme combines DAS and Story schemes to provide authenticity to the user for securing the system.

Bin B.Zhu ,Jeff Yan [5].In this paper a new security primitive relying on unsolved hard AI problems.The CaRP introduces a new approach to graphical passwords which adopts a online guessing attacks.CaRP will solve the AI problems. Hpwever, a password is more valuable to attackers and hackers than a free email account that captcha is used to protect in it.Since, it is more tough for the attackers to hack CaRP than Captcha.

Joseph Bonneau[6] proposed a technique where graphical and cognitive schemes offer some improvements in passwords and is displaced it by the another one. Some schemes do better and some worse where user have to work harder to improve it. The inventors will make a approach where passwords tend to come from the security community.

There is a graphical password technique which is made up of handwritten designs or text that is normally drawn from a stylus onto a touch screen in a system. According Jermyn et al. [7] it is very tougher to crack the doodle password because they are having a theoretically much larger number of possible doodle passwords than a text passwords in it. It is not used as much because it has problems with the recognition.

The Syukri algorithm proposes a system where authentication is gained by the user using a mouse to draw his signature as it also be proposed by Di et al [8]. This technique is consists of two stages, firstly registration and other is verification. To start with, during the registration stage the user have to send request to draw his signature with a mouse, after that it is followed by the system extracting the signature area and either enlarging or scaling-down signatures, and rotating if it is required, (also known as normalizing). However, the information is stored into the database. The verification stage is now begins where it is obtaining the user input, on which this will repeats the normalization factor and ; thereafter it extracts all the parameters of the signature in it. Basically, the system will uses the geometric average means and a dynamic update of the database for a verification purposes. Based on the study of Ali, in 2008 undertaken, the graph of successful verification was satisfying here. The major benefit of this approach is that not only is there no requirement for memorization of one's signature but also counterfeit the signatures which is difficult to come up with.

Greg E. Blonder [9] proposed this method in 1996. To begin with a pre-determined images is presented to the user on a visual display or in his system and then the user is supposed to tap regions of an images by pointing to one or more predefined locations on the image in a predetermined order of pointing out his or her authorization to access the resource. According to Blonder this method is secure since it has a million of different regions to pick from the images. The main drawback to this scheme was that the amount of predefined clicks in this regions was relatively so small so as the password had to be quite long and spacious in order for it to be secure

In 2005, Pass Point was created, as it will fulfill all the shortcomings of an algorithm of a Blonder. Pass point was able to fill in the gaps left by the blonder. Here, the image can be any natural picture or painting where there is having a several possible click points. Apart from this, the image is not to be secret and has no other work other than that of assisting the user to memorizing the click point. Furthermore it is not as rigid as the blonder algorithm which requires all the setting of a artificial predefined click regions with all well marked boundaries. The authentication process will involves the user have to select (Lashkari et al.[10]) several points on picture in a predetermined order.

When logging in, the user is supposed to be click close to the selected click points, within some (adjustable) tolerance distance, for instance within 0.35 cm from the actual click point in it.

DOI 10.17148/IJARCCE.2015.43138

Passlogix Inc.[11] is a New York City USA based commercial security company which has created a scheme called Passlogix v-Go. Its approach to as "Repeating a sequence of actions" which implies that a password is created by following a predefined order. In this scheme, a user have the option of choosing their preferred background images based on the environment, such as the park ,house, school . By clicking and/or dragging on a number of items within that image, a user is able to input their password in to that image. In this event the environment opted for by the user is the school environment, the user can choose a set of books and objects regarding study, for them it can be any of it, where he can select one particular thing in that image.

IV. PROPOSED SYSTEM

This paper proposed a new algorithm for encryption of data that is "Steaganography" that encrypts alphabets in to a image which will be hidden inside in it. There is an authentication scheme for a graphical password where it will infeasible to the most popular attacks shoulder surfing and image gallaery attack. There is having a matrix of images in it, where there is having some code written below each image which is randomly changed while logging.

This can be view to the user while log in the page and during registration in it. There is having some code is hidden in that images and it will not be visible to the user. While registration user have to select that images as his password, where the data that is hidden beyond that images will store into a database and it will be invisible to the user. It is the better way of resisting and countering the shoulder surfing and image gallery attacks. Here, a user can use any crypto technique for hiding the data into a images in it. The main focus is on the attacks of graphical password algorithms and how it can be evaluated in it. Finally, it will determine the resistance of a algorithm on common password attacks and their evaluation.

V. CONCLUSION

There are many authentication schemes in the current state. Some of them are based on user's physical and behavioral properties, and some other authentication schemes are based on user's knowledge such as textual and graphical passwords. After this a GUA attack patterns survey was done in an attempt to make a comparison table for recall-based algorithms based on attack patterns. Since there is no proper evaluation framework for GUA algorithms until now, we focus on attacks of graphical password algorithms and evaluate all recognition based algorithms.

Then, after explaining the various crypto techniques and schemas, this is a new graphical password algorithm that uses steganography techniques and random character set to provide stronger security against image gallery attacks and shoulder surfing attack. As part of future works, an algorithm that is resistant to most of the shortcomings mentioned in this paper will be proposed and developed.

ACKNOWLEDGMENTS

We would like to express our appreciation to our parents and all the teachers and lecturers who helped us to understand the importance of knowledge and show us the best way to gain it.

REFERENCES

[1] Gao, H., et al., A New Graphical Password Scheme Resistant to Shoulder-Surfing, in International Conference on Cyberworlds. 2010, IEEE: Singapore p. 194 - 1999
[2] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Survey"s, vol. 44, no. 4, 2012.
[3] Hasegawa, M., Y. Tanaka, and S. Kato, A Study on an Image Synthesis Method for Graphical Passwords, in International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS 2009). 2009.
[4] Gao, H., et al., Analysis and Evaluation of the ColorLogin Graphical Password Scheme, in Fifth International Conference on Image and Graphics(ICIG). 2009, IEEE. p. 722 - 727
[5] 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.
[6] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. van Oorschot, "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism," IEEE Trans. on Dependable and Secure Computing, vol. 9, no. 2, pp. 222–235, 2012.
[7] F. Stajano, "Pico: No more passwords!" in Proc. Sec. Protocols Workshop 2011, ser. LNCS, vol. 7114. Springer.
[8] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years," ACM Computing Surveys, vol. 44, no. 4, 2012.
[9] J. Bonneau, "The science of guessing: analyzing an anonymized corpus of 70 million passwords," IEEE Symposium Security and Privacy, May 2012.
[10] Lashkari, A.H., et al., Shoulder Surfing attack in graphical password authentication. International Journal of Computer Science and Information Security, 2009. 6(9).
[11] Sandouka, H., A. Cullen, and I. Mann, Social Engineering Detection using Neural Networks, in 2009 International Conference on CyberWorlds 2009, IEEE.
[12] Kumar, M., et al., Reducing Shoulder-surfing by Using Gaze-based Password Entry, in Symposium On Usable Privacy and Security (SOUPS). 2007: Pittsburgh, PA, USA
[13] S.Drimer, S. J. Murdoch, and R. Anderson, "Optimised to Fail: Card Readers for Online Banking," in Financial Cryptography and Data Security, 2009, pp. 184–200.
[14] A. Pashalidis and C. J. Mitchell, "Impostor: A single signon system for use from untrusted devices," Proc. IEEEnGlobecom, 2004.
[15] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in Proc. Symp. Usable Privacy Security, 2007, pp. 20–28.
[16] 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.

DOI 10.17148/IJARCCE.2015.43138