International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

Graphical User Authentication Using Random Codes

Mr.D.S.Gawande[1], Manisha P. Thote[2], Madhavi M. Jangam[3], Payal P. Khonde[4], Payal R. Katre[5], Rohini V. Tiwade[6]

[1]Assistant Professor, Computer Science and Engineering, DBACER, Nagpur, Maharashtra, India
[23456]UG Student, B.E., Computer Science and Engineering, DBACER, Nagpur, Maharashtra, India

---

Abstract - *Now a days user authentication is one of the most important topic in information security . In this project, we propose a new graphical password scheme for authentication. Here user selects number of images as a password and while login user needs to enter the random codes generated below each image, which has been set as a password. The GUA (Graphical User Authentication) or simply Graphical based Password on the fact that humans tend to remember images better. This type of interface provides an easy to create and remember passwords for the users. This Scheme provides a way of making more user-friendly passwords. Here the security of the system is very high and every time user needs to enter different set of random codes for authentication i.e. every time new password gets generated for every login attempt. Dictionary attacks, Brute Force attack, shoulder surfing attack and spyware attack are infeasible on this password scheme.*

***Key Words*: Graphical password, authentication, security, random codes, shuffling**

1.INTRODUCTION

Most of the graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are abundant with both usability and security problems that make them less than desirable solutions. Graphical passwords also reduce the memory burden on users, coupled with a larger full password space offered by images and more secure passwords can be produced and users will not resort to unsafe practices in order to cope.

Now a days security has become an important issue in today's world. To enforce security of information passwords were introduced. Graphical passwords are introduced as an alternative technique to textual password. Therefore we need supplements for traditional methods to have more reliable and secure authentication. Graphical authentication schemes allow user many choices while it influencing users towards stronger passwords. This project proposed a mechanism of Graphical Authentication using random codes which deals with graphical images with the help of random codes. Here random codes are alphabetic characters which randomly appears. The most common authentication method of alphanumeric as a text based password has proven difficult for the user to remember the password. The attacker can also easily guess the text based password. This is a user friendly authentication mechanism using random codes where human need not to remember text. Since, it is easier for human to remember pictures. It also offers protection against relay attacks such as Brute force, dictionary attack, shoulder surfing attack etc. The aim of this project is not only provide security but also make more user friendly mechanism. Graphical authentication using random codes may prove to be superior to the text as well as graphical based password. A graphical password is an authentication system that works by selecting the images by the user, in a specific order (GUI). For this reason, the graphical-password approach is called graphical user authentication .A graphical password is easier than a text-based password for most people to remember. Graphical passwords may provide more security than text-based passwords because many people cannot memorize text-based password

2. RELATED WORK

2.1 Dhamija and Perrig Technique :

[1]This technique proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity. In this system, during registration the user selects a certain number of images from a set of random pictures. Later, during login the user has to identify the pre-selected images for authentication from a set of images as shown in figure 1. This system is vulnerable to shoulder-surfing attack.

Fig -1: Random images used by Dhamija and Perrig

2.2 Passface Technique :

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

Fig -2: Examples of Passfaces

2.3 DAS Technique :

[3]This technique proposed a new technique called "Draw-a-Secret" (DAS) as shown in figure 3,where the user is required to re-draw the pre-defined pictures on a 2D grid. If the drawing touches the same grids in the same sequence, then the user will authenticated. This authentication scheme is vulnerable to shoulder surfing attack.

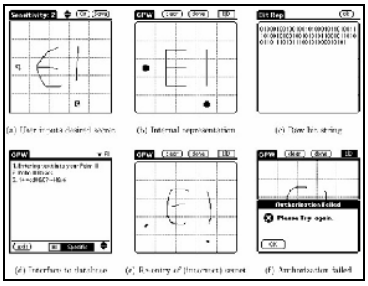

Fig -3: DAS technique by Jermyn

2.4 Haichang's Shoulder Surfing Technique :

[4]This technique proposed a new shoulder-surfing resistant scheme as shown in figure 4,where the user is required to draw the curve across their password images orderly rather than clicking on them directly. This graphical scheme combines DAS and Story schemes to provide authenticity to the user.

Fig -4: Haichang shoulder-surfing technique

3. ATTACKS

The following attacks are removed in this project i.e graphical user authentication using random codes

3.1 Dictionary attacks

Although recognition based graphical passwords have mouse input instead of keyboard input, it will be inconvenient to accomplish dictionary attacks against this type of graphical passwords. For some recall based graphical passwords, we can use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack.
We believe text-based passwords are more vulnerable to dictionary attacks than graphical passwords.

3.2 Guessing

Unfortunately, graphical passwords are often predictable, a serious problem arise associated with text-based passwords. For example, study on the Passfaces technique have shown that people usually choose weak and predictable graphical passwords. Nali and Thorpe's have studied similar predictability among the graphical passwords created with the DAS technique. More research is needed to understand the nature of graphical passwords created by real world users.

3.3 Spyware

Except few exceptions, key logging and key listening spyware cannot be used to break graphical passwords. It is not clear that "cursor tracking" spyware will be more efficient tool against graphical passwords. However, mouse motion itself is not enough to break graphical passwords. Such type of information has to be correlated with application information, such as window size , position and timing information.

3.4 Shoulder Surfing

As similar to text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only some recognition-based techniques are designed to defy shoulder-surfing. None of the recall based techniques are considered as should-surfing resistant.

4. PROPOSED PLAN

4.1 HIDING SECRET CODES IN IMAGES:-

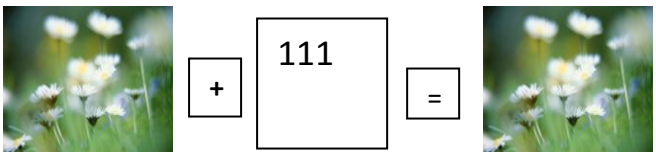

Fig -5: Data hiding

The least significant bit (LSB) algorithm is used to hide a code into the image. In this project a numeric code is hidden in the image using least significant bit (LSB) algorithm. The code hidden image is displayed on the login screen. The code is used to compare the user selected image in back end. The code is extracted from the image to match the code with the code already stored in the database. This helps to identify the users image and then the user will login. Above fig(e) shows how data hiding is performed. Firstly select a image and a numeric code .then apply Least Significant Bit algorithm to hide that code into the image. The Least Significant Bit (LSB) insertion method is a common and easy method for embedding information in a graphical image . In LSB insertion method every pixel is replaced by every message bit. Also, the change occurs only in the bit which is least significant, thus keeping the other more significant bits unchanged. It does not affect the original image perceptibility. Hence it is a very popular technique. LSB technique can be use wherever we want to store confidential information on a standalone PC or one which is shared among various users. LSB technique can be used to store any data such as ATM PIN, Credit card details, salary statement etc. So, wherever such kind of information is to be preserved in a manner that only allowed user should be able to retrieve the data whenever needed, by simple ways, LSB is a better solution. Least Significant Bit (LSB) encoding is the easiest of the techniques used for embedding secret or confidential information in images. For a grey scale bitmap , using the LSB of each byte in an image, a secret message of the Cover image can be stored. This can be easily done by substituting every bit of the secret message into every LSB.

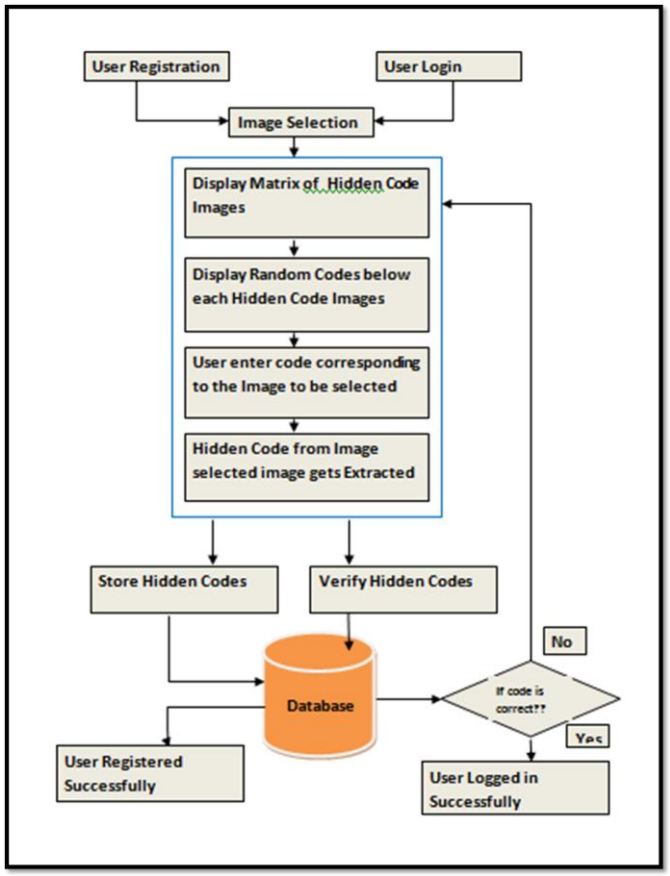

Fig -1: System Architecture

4.2 Registration phase

In registration phase , the image matrix contains the password. User can select some images from the matrix as password by entering the code the corresponding image and submit to the system, for example user select any number of images as the password.

Once the user selects the preferred password, the users string will be generated. For example, a user selects three images as the preferred password with corresponding code below the image as 'mnp' & 'pbu' &'xyz' and these images has a hidden code embed in the images as 1050 ,4578 and 7528. Now as soon as the user enters the code in the form 'mnppbuxyz' and click on submit button, the algorithm will first split the password string into a string of 3 characters and will store the string in a list. Now it will check for the image on the image matrix having corresponding code as 'mnp'. Once it finds the exact match of the image, it will extract the hidden code from the image i.e., 1050 and will store the user ID and the extracted code into the database. Same steps will be repeated for the next string also and thus completing the registration process.

The workflow of registration phase is as below:

Step1: User clicks on registration button.

Step2: In registration page, the user has to enter User ID and Select the password.

Step3: User have to select the password image by entering the random code generated below the image.

Step4: Algorithm checks for the match of code entered by the user and its corresponding image.

Step5: Extract the hidden code from the image.

Step6: Store the hidden code and the User ID into the Database.

4.3 Login phase

In the login section, the user first enters his username. The image matrix will be displayed which will contain same images as we had in the registration form but the position of the images will be different. Again each image will have some random characters below it. The user should recognise his password images and then enter the text corresponding to his password image in the password textbox. Now Algorithm will again split the string into sub strings of 3 characters each. Here the algorithm will then find the related images of the entered characters from the login matrix. After finding the images associated with entered characters, algorithm will extracts the hidden data from the database and checks the data with the user information and if the information is same then user can login to the system, otherwise, the user need to try again.

The workflow of Login phase is as below:

Step1: User will click on Login button.

Step2: In Login page, the user have to enter the User ID and password.

Step3: User enters the password by entering the code generated below the password image.

Step4: Algorithm checks for the match of code entered by the user and its corresponding image.

Step5: Extract the hidden code from the image.

Step6: Checks weather the code extracted from the image selected by the user belongs to the User.

Step7: If yes, user gets Login else needs to enter the password again.

5. CONCLUSIONS

In the field of information security, user authentication is the most critical of all the elements. Researches has shown that people have to remember combinations of patterns, geometrical shapes, colours and textures better than alphanumeric passwords that are meaningless to the user. This proves that graphical password is a more desirable alternative to text based passwords. At the beginning of this paper, we presented the recognition based algorithm type of graphical password. Since there is no proper evaluation framework for GUA algorithms until now. This mechanism generates different password & that are resistant to dictionary attacks, brute Force attack, and shoulder surfing attacks.

We are providing more user friendly passwords as user do not need to remember the graphical password .Finally, we evaluated this proposed algorithm and its working for securing the web account access..

REFERENCES

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

[2] Real User Corporation: Passfaces. www.passfaces.com

[3] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin. “The design and analysis of graphical passwords” in Proceedings of USENIX Security Symposium, August 1999.

[4] HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing"

[5]IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014 891

Captcha as Graphical Passwords—A New SecurityPrimitive Based on Hard AI ProblemsBin B. Zhu, Jeff Yan, GuanboBao, Maowei Yang, and NingXu

[6]] Lashkari, A.H., et al., Shoulder Surfing attack in graphical password authentication. International Journal of Computer Science and Information Security, 2009. 6(9).

[7] 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

[8] Sandouka, H., A. Cullen, and I. Mann, Social Engineering Detection using Neural Networks, in 2009 International Conference on CyberWorlds 2009, IEEE.

[9]M.sreelatha,Authentication schemes for sessional password using color and images . International journal of

network security and its application(IJNSA),vol .3,No.3,May 2011.

[10]] 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.