Securing an Graphical Password by multiple questions and random codes

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

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

Abstract--This paper presents a authentication technique where it is having an secure way of hiding the data from hackers and unauthorized user. Here, it will create a different barriers for the hacker so that he may get confused to hack the secure data of the account. There is a critical problem about hacking of data in a networking world. So, to prevent that hacking here it will create a image based password where there is having a random codes below the images in a gallery so that it cannot be copied by any user, and mainly it will prevent the shoulder surfing attack which is very popular nowadays. The images are displayed in a gallery according to the choice of an user interest where he will choose his question and according to that question the relevant images are displayed in it. As it will provide the security to the user's account while logging his account. There is no chances of proxy password in a login page ,it will capture easily the attacker and block the account. As, it is resistance to all types of attacks and mainly it will provide a excellent security to the user's information. It is better than a textual based password and prevents the image gallery attack.

Keywords-Graphical Password ,Authentication Security ,Shoulder surfing ,image gallery attack

I. INTRODUCTION

Graphical password are generally more easier to remember than textual based passwords and it is a human tendency that he can write a same password for different accounts. So, that there are possibilities of hacking the password very easily by different software like key-loggers. It will easily capture the code that will user set it as his or her password. To prevent all such types of attacks , this paper introduced a new technique of authentication where user gets more security to hide his information in a proper way from different hackers and other users. There are many papers where authentication is done in a different ways but it will not infeasible to shoulder surfing attacks. Here, by studying all the papers and finding all the problems in it, tried a new technique where all the data will be kept hidden and to prevent it from hackers. Mostly people uses a textual based password but it is not secure for them to secure their information. So, graphical password is to be generated to stop that attacks. And in textual based password there are different attacks were occurs like brute force, guessing attack, dictionary attacks. And it will create a problem for the user to sign in his account by using text based password. For this reason this graphical password scheme is created to prevent it from all difficulties of different attacks. Likewise , there are only two attacks are possible in a image based password and here we will also makes infeasible to this two attacks. So, that there are very few chances of attacking the image gallery and finding a password. As, to make all suggestions from different authors of graphical password papers, it will conclude that this paper is infeasible to any attacks in it.

II. AUTHENTICATION

In day to day life, there are several things that we want to make secure it from others. In this type there is an authentication scheme which will provide security to our information which is called as authentication. This is the process of securing the data from threats to remain its privacy and here the user will grant permission's to access the resources. User authentication mostly occurs with the interaction of human to computer. Mostly, a user have to enter the username and password to begin his system. There is some authorization which provides online backup services, updating and

ISSN: 2278 – 1323

monitoring systems to securely authenticate and verify the system in a way that it is not a hacker. User names are generally being their initials which makes them easy to guess. people often create weak passwords, which are easily stolen. There are certain assumptions in it like minimum length, complexity, and some special symbols which are more vulnerable to different attacks. In authentication it is defined as a system which will consists of different challenges and tasks to response. There are various factors which will depend up on strong security, ATM machines, banks used that password scheme to protect from different threats. Authentication will be done in a way that no one can stolen it, and not easily accessed by any other.

III. RELATED WORK

There are different authentication techniques which are to be done by different authors. In recognition based technique[1] there are several images in a gallery, where user have to select the different images according to his choice in it. He will pick several pictures from the gallery and after that set it as his password. But there is a drawback of that technique which takes longer to create than text password, and creates heavy load on database to store many images because there are unlimited images in it.

In Passface technique[2] , there are several images of faces which are to be registered in an account by selecting those images as its password. This faces are to be selected by the user's choice where it will be having an different faces in it. There is an disadvantage is that there is having a heavy load in database of that decoy images in it. And sometimes it is predictable also.

Man-et-al [3] proposed a technique of an pre-registered picture objects in a gallery which are fixed and while login the page user have to write a code written below each picture and set it as his password. But it is difficult for the user to remember the codes written below the picture and the images in it.

IV. PROPOSED SYSTEM

This paper proposed a method where it will consists of different images in a gallery and it is mainly feasible to shoulder surfing and images gallery attacks that will not possible in textual based password. As, it is having an authentication scheme, where it will be having an different questions will be set according to user's choice where user select his or her own question and according to his choice he will be displayed a number of images in it, where there is some code written below every image in a gallery. And while login the account, user have to first fill all his details in it.

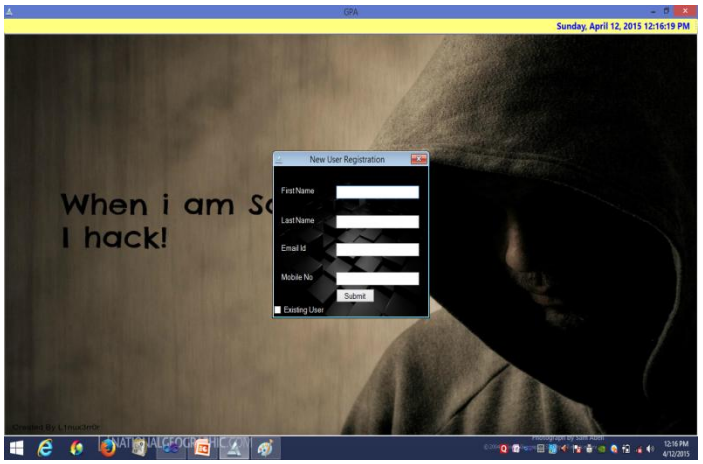

Fig 1: Registration of an account

After filling all the details in it, user have to move to the image gallery and a question port where he will get different questions and according to user's choice he have to select one of the question in it. Then, he will get a relevant images according to his choice of a question.

Likewise, in this paper it will consists of different questions and according to his images are in the gallery. The codes that are below each image are randomly changing. If user want to login his account next time he just have to remember the images that he had selected during the registration phase and write a code in a password box in it.

ISSN: 2278 – 1323

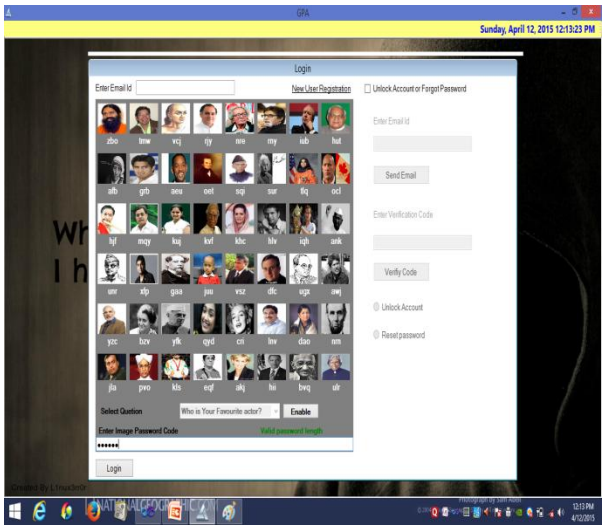

Fig 2: Selection of question in a image gallery

Registration will be done in a way that user can remember the image that he had selected and it will infeasible to the shoulder surfing attack because if anyone can capture his password there will be no use as everytime codes will be changing below each image and also changing their positions. If user want to change his password then there is a option for reset the password where he will select the question and set an images as his password. There is having another alternative if user wants to lock his account he can do it and also he can unlock his account when he wants. If user forget his password then he have to click on forget password where he have to enter his email id and after that he will get a code in his mail where he have to enter that code in box verify code and after that he will get the login and according to procedure he will select the desired question that he wants. It is better way of countering the different graphical passwords attacks in it and it is resist to all attacks. It will be shown that text based passwords are more complicated and it is easily captured by anyone, as compared with graphical based password.

V. CONCLUSION

There are many authentication schemes in this area of networking world. Here, some authentication schemes are based on the physical and behavioural structure, and some other authentication schemes are based on user's knowledge such as textual and graphical passwords. As, we know that text based passwords are often difficult to remember because it will consists of special symbols, capital and small letters in it. This is infeasible to all the attacks shoulder surfing and image gallery attack which are very popular nowadays. This authentication technique provides more security to the information that we want to keep secret in our system and it is infeasible to all the attacks in it.

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.

ISSN: 2278 – 1323

[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.

ISSN: 2278 – 1323