A Shoulder Surfing Resistant Graphical Authentication System

Poornima Hotagi [1], Sunanda Biradar [2], Sanjeevini hotkar [3], Pooja Halakurki [4], Revati Lalasangi [5]

[1] Department of Computer Science and Engineering, BLDEA's V.P. Dr. P.G.H College of Engineering and Technology,Vijayapur, 586103, India; poornima.hotagi@gmail.com
[2] Department of Computer Science and Engineering, BLDEA's V.P. Dr. P.G.H College of Engineering and Technology,Vijayapur, 586103, India; sunanda_biradar@rediffmail.com
[3] Department of Computer Science and Engineering, BLDEA's V.P. Dr. P.G.H College of Engineering and Technology,Vijayapur, 586103, India; sanjeevinihotkar@gmail.com
[4] Department of Computer Science and Engineering, BLDEA's V.P. Dr. P.G.H College of Engineering and Technology,Vijayapur, 586103, India; poohalakurki21@gmail.com
[5] Department of Computer Science and Engineering, BLDEA's V.P. Dr. P.G.H College of Engineering and Technology,Vijayapur, 586103, India; revatilalasangi@gmail.com

ABSTRACT

Graphical password has more secure compare to the textual passwords. Graphical Authentication password is widely used in many applications for high security purpose. Most of the authentication system is a combination of username and password for authentication. Which is done Using the images that split into equal square blocks, user select only one block per image.

Key Words: Graphical password, Authentication, Security, Textual password.

1. INTRODUCTION

Textual passwords are week due to the difficulty of maintaining strong ones. If user try to maintain strong one it's not possible to catch up and recall them. Various graphical Password authentication schemes were developed to address the problems and weaknesses associated with textual passwords. The paper covers the graphical password using matrix form. The image is divided into 5x5 grid. The image contains 25 blocks ranging from (0-24). Anyone can be selected and used to login into user account. Shoulder surfing is nothing but when user enter the textual password, hacker will observe without knowing to the user.

2. LITERATURE SURVEY

In [1], authors address the problem regarding authentication in the mobile devices specially about the latest device (touch screen devices like mobile, iPad, notepad and so on. The attack Especially on mobile touch screen when the user draws the pattern to open the mobile. In [2], authors address Draw-A-Secret password schemes, to draw the signature of user for authentication, and uses the Draw -A- Secret (DAS) method where user draw the signature on the 2D grid for security purpose. In [3], authors address a database containing data from 120 users taken with a touch screen mobile device. The data contain information about signature. In [4], authors address about the component of the security and Provide the interface to access the login information of the user. It includes login information and graphical password information. Here we are choosing entire image as password. In [5], authors address about the more secure textual password proposed by graphical password authentication using the color scheme. Analyze the shoulder surfing during the login. For better usability and accessibility. In [6], authors address Information security in online services and web applications such as social media applications (Facebook, Twitter, Banking, Online Examination. etc.). This is done by using captcha as graphical password authentication.

3. PROPOSED SYSTEM

In proposed system we choose the image block from the selected image. The image is divided into 5x5 grid. Graphical passwords refer to using the images (also drawings), graphical passwords can be easily remembered, as users remember images better than words. Also, they should be more resistant to brute-force attacks because there is practically an infinite search space. Graphical passwords techniques are categorized into two main techniques: recall-based and recognition-based graphical techniques.

- **Recognition Based System:** In recognition-based techniques user should try to remember the block selected and has the unique ability to identify the image selected during the registration phase. Once user recognize the image can log into account easily rather than remembering big textual password of some length.

DOI : 10.18231/2454-9150.2018.0226

• **Recall Based System:** In this technique, a user recalling something that created or selected earlier during the registration step. Only after recalling the image and block division user will be able to login in into the account it's not possible to access the information until the admin give the authorization.

Dividing Image into Equal Square jQuery is platform used for scripting client-side html pages. the to the jQuery library allows the creation of animated web pages and Web applications. Here we have BlockID, ImageID, blockAddr, where ImageID equal to the image, BlockID contains block value, and blockAddr contains ImageID plus BlockID. $.fn.splitIntTiles function is used to split the images into equal square. The divided image is shown in Figure 1.

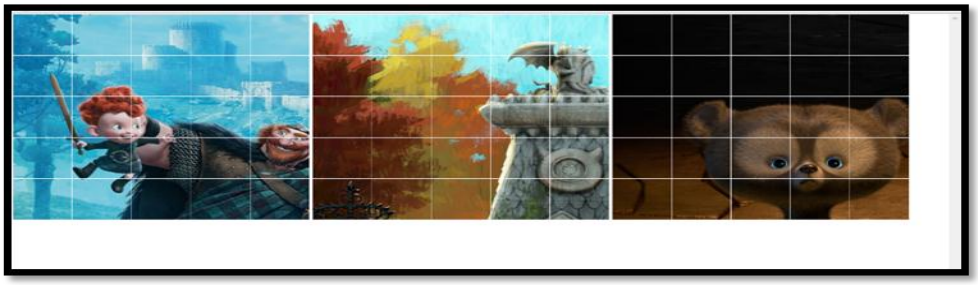

Figure 1: Dividing the image into equal parts

Here we will select only one block from any of these 3 images. The block chosen during registration will be used while user login into an account. After login do the operation which was stated above.

4. IMPLEMENTATION OF THE SYSTEM

There are two types of user login modules implemented; namely, admin and user module.

4.1. Admin Module

In this module, admin has secure username and password. After login successful admin can do some operations such as view all user, their details and authorize them, upload the documents with image and view all uploaded documents with rank and contents of it, view the documents results based on rank.

4.2. User Module

In this module, there are thousands of users. After registration successful user can login by using valid user name and password and also by using graphical method. After successful login user can do operation like View Profile, Search Document, View Recommended Documents.

5. CONCLUSION

Textual passwords were widely used compare to the graphical password. But still graphical password provides more security for many applications. The application of graphical password can be used in social sites, bank system, hospital system etc.

REFERENCES

1. Oakley and A. Bianchi, *Multi-touch passwords for mobile device access*, In Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. Ubi Comp '12. New York, NY, USA: ACM, 2012, pp. 611–612.
2. M. Martinez-Diaz, J. Fierrez, and J. Galbally, *Graphical password-based user authentication with free- form doodles*, IEEE Transaction son Human-Machine Systems, vol. 99, pp. 1–8, 2015.

A. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith*, Smudge attacks on Smartphone touch screens*, in USENIX 4th Workshop on Offensive Technologies, 2010.

3. Zhao and X. Li, *S3pas: A scalable shoulder surfing resistant textual-graphical password authentication scheme*, in Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 467–472.
4. Ahmad Almulhem*, A Graphical password authentication system*, Access IEEE, World Congress On Internet Security(Worldcls-2011),2011.
5. Vikas K. Kolekar; Milindkumar B. Vaidya, *Captcha as graphical password authentication schemes for smart phone and web,* International Conference on Information Processing(ICIP), Dec 2015.

DOI : 10.18231/2454-9150.2018.0226