ISSN: 2319-6505

Available Online at http://journalijcar.org

International Journal of Current Advanced Research
Vol 5, Issue 10, pp 1362-1363, October 2016

RESEARCH ARTICLE

International Journal of Current Advanced Research

ISSN: 2319 - 6475

MULTI-TYPE GRAPHICAL AUTHENTICATION FOR ORGANIZATION

Kirthika S and Shenbagavalli R

Krishnasamy College of Engineering & Technology, Cuddalore, Tamil Nadu

ARTICLE INFO

Article History:

Received 9th July, 2016
Received in revised form 5thAugust, 2016
Accepted 28th September, 2016
Published online 28th October, 2016

Key words:

Character recognition, Graphical captcha, Image pixel selection, image Orientation, Image comparison, Security.

ABSTRACT

Sensitive data like passwords which is suspected to be infected with spyware which snoops on the user's activity. Securing data became a major role in today's technological world. Thereby, different techniques are used to make the data more secure. To make user authentication more secure by avoiding alphanumeric string which users tend to choose passwords either short or meaningful for easy memorization. To overcome this problem, we proposed a novel authentication system with five different authentication methodologies: I) Random pixel selection. II) Password draw method (character recognition). III) Numeric authentication (password selection using arrow key). IV) Oriented image selection. V) Image comparison using image features. We implemented various authentication in banking sector proposed system achieves better resistance to spyware attacks while maintaining usability.

© Copy Right, Research Alert, 2016, Academic Journals. All rights reserved.

INTRODUCTION

TEXTUAL passwords have been the most widely used authentication method for decades. Comprised of numbers, upper- and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect. Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings [1]. We present a secure graphical authentication system to protect users from becoming victims of surfing attacks when inputting passwords in public through the usage of one-time login indicators.

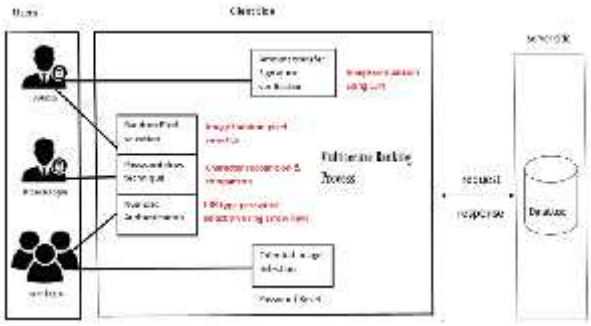

Fig.1 Secure banking with multi authentication technique.

Random pixel selection

To overcome the security weakness of the traditional PIN method, the easiness of obtaining passwords can be observed in public, and the compatibility issues to devices arises. Thereby, graphical authentication system called Pass Matrix is used. In Pass Matrix, a password consists of only one pass-square per pass-image for a sequence of n images. The number of images (i.e., n) is user-defined. Below figure demonstrates the proposed scheme, in which the first pass-square is located at in the first image, the second pass-square is on the top of the smoke in the second image at, and the last pass-square is at in the third image. In Pass Matrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the Pass Points scheme [2].

Fig.2 The pass squares are shown in the orange filled areas in each image

Image feature comparison

LOCAL DIRECTIONAL NUMBER PATTERN -The proposed Local Directional Number Pattern (LDN) is a six bit binary code assigned to each pixel of an input image that represents the structure of the texture and its intensity transitions. The positive and negative responses provide valuable information of the structure of the neighborhood, as they reveal the gradient direction of bright and dark areas in the neighborhood. Thereby, the distinction between dark and bright responses allows LDN to differentiate between blocks with the positive and the negative direction swapped (which is equivalent to swap the bright and the dark areas of the neighborhood, by generating a different code for each instance, while other methods may mistake the swapped regions as one[3][4]. Furthermore, these transitions occur often in the face, for example, the top and bottom edges of the eyebrows and mouth have different intensity transitions.

Fig.3 Image feature comparison sample

Password draw method

The graphical capability of handheld devices was weak and the color and pixel it could show was limited. Under this limitation, the Draw-a-Secret (DAS) technique where the user is required to re-draw a pre-defined picture on a 2D grid. If the drawing touches the same grids in the same sequence, then the user is authenticated. Since then, the graphical capability of handheld devices has steadily and ceaselessly improved with the advances in science and technology [7].

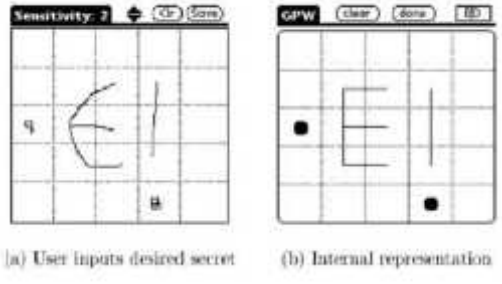

Fig.4 Draw a secret sample

Oriented image selection

Click-based graphical CAPTCHA is user friendly as the user is fond of images. In addition, a refresh button will be provided where the user gets a new graphical CAPTCHA if he is not able to understand the present CAPTCHA. The Click-based graphical CAPTCHA is posed to the user when the user wants to login to the website [5][6]. To authenticate and verify a user, the user needs to go through the following two phases-Registration Phase and Login Phase.

CONCLUSION

A user can be given access to secure systems based on user credentials that imply authenticity. A network administrator can give a user a password, or provide the user with a key word or other access device to allow system access [8]. Thereby, different techniques and the input of authenticity can help to secure data. Therefore, by using graphical authentication we can provide a secure system and be free from fraud and other malpractice.

References

1. J. Long and K. Mitnick, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Elsevier Science, 2011.
2. Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, *A Shoulder Surfing Resistant Graphical Authentication System,* PP. 99, 2016.
3. Manjunatha S B, Guruprasad A M, Vineesh P, *Face Analysis By Local Directional Number Pattern, International Journal of Engineering Research and General Science* Volume 3, Issue 1, January-February, 2015, ISSN 2091-2730.
4. Z. Xie and G. Liu, —Weighted local binary pattern infrared face recognition based on weber's law, ‖ in Image and Graphics (ICIG), 2011 Sixth International Conference on, Aug. 2011, pp. 429–433.
5. C.Shoba Bindu, *Click Based Graphical CAPTCHA to Thwart Spyware Attack*, IEEE International Advance Computing Conference (IACC) 2015, pp.324-328.
6. Haichang Gao, Honggang Liu, Dan Yao, Xiyang Liu, Uwe Aickelin, *An audio CAPTCHA to distinguish humans from computer*, Proceedings of the Third International Symposium on Electronic Commerce and Security, 2010.
7. S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), International Conference on, Jan 2014, pp. 479–483.
8. I. Oakley and A. Bianchi, "Multi-touch passwords for mobile device access," in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. UbiComp '12. New York, NY, USA: ACM, 2012, pp. 611–612.

****