International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 5 – APRIL 2017.

DESIGN OF AUTHENTICATION SYSTEM USING MULTIMEDIA FOR BETTER SECURITY

P. Priyanka[#1], M. Yohithapandi[#2], M. Vijayalakshmi [#3] and A. Subinamary[#4]

[#] *Bachelor of Engineering in Computer Science Engineering, N.P.R. College of Engineering and Technology, Dindigul, India*

***Abstract*— Authentication based on passwords is widely used in applications for computer security and privacy. However, human actions such as choosing bad password and inputting password in an insecure way are regarded as "the wreaked link" in the authentication chain. Other than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications anytime and anywhere with various devices. This improvement brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect user's credentials.**

To solve above problem, we are using a novel authentication system Pass Matrix, based on graphical password to resist shoulder surfing attacks. With a onetime valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix offers no hints for attackers to figure out or narrow down the password even they conduct multiple camera based attacks. We also implemented a Pass Matrix prototype on android and carried out real user experiments to evaluate this memorability and usability. From the experimental result the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.

***Index Terms*— Click Points, Application Programming Interface, Sound Signature Frequency**

I. INTRODUCTION

Textual passwords have been the most widely utilized validation technique for decades. Comprised of numbers furthermore, upper-and lower-case letters, textual passwords are viewed as sufficiently solid to oppose against brute force attacks. A solid textual secret password is difficult to retain and remember. In this manner, users have a tendency to pick passwords that are either short or from the word reference, rather than irregular alphanumeric strings. Far and away more bad, it is most certainly not an uncommon case that users may utilize one and only username and password for different account. As indicated by an article in Computer world, a security team at a large organization ran a network password cracker and shockingly split around 80% of the employee's passwords inside 30 seconds. Textual passwords are frequently insecure due to the trouble of maintaining up solid ones. Varient graphical password validation schemes were produced to address the issues and shortcomings connected with textual passwords. In view of a few concentrates, for example, people have a better capacity to remember images with long-term memory (LTM) than verbal representations. Image based passwords were ended up being simpler to recall in a few user ponders. Accordingly, users can set up a complex authentication password and are fit for remembering it after quite a while regardless of the possibility that the memory is not activated periodically.The greater part of these image based passwords are helpless against shoulder surfing attacks (SSAs). This sort of attack either utilizes direct perception, for example, viewing over somebody's shoulder or applies video catching methods to get passwords, PINs, or other sensitive individual data.

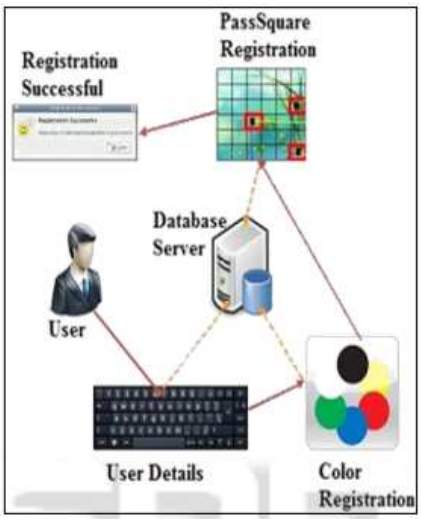


Fig.1. Registration System

The human activities, for example, picking bad passwords for new account and inputting passwords in an unreliable way for later logins are viewed as the weakest link in the validation chain. Hence, an authentication scheme ought to be intended to overcome these vulnerabilities.

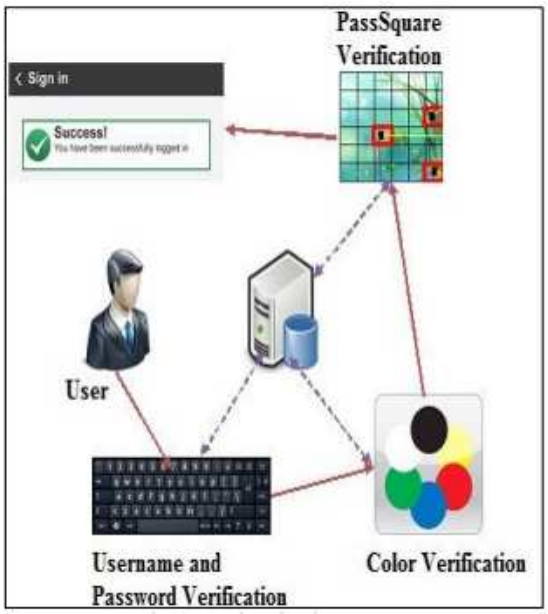


Fig.2. Authentication System

Most human activities are give bad passwords for new account and inputting passwords in an unreliable way for later logins are viewed as the weakest link in the validation chain. Hence, an authentication scheme ought to be intended to overcome these vulnerabilities.

A graphical password system is a supportive sound signature to increase the remembrance of the password is discussed. In proposed model a click-based graphical password scheme called Sequence of juncture image is presented. In this model a password consists of sequence of some images in which user can select one click-point per image. In addition user is asked to select a sound signature corresponding to click point this sound signature will be used to help the user to login. Model showed very good Performance in terms of speed, accuracy, and ease of use. Users preferred Sequence of juncture image to Pass Points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points.

Passwords are used for – (a) Authentication (Establishes that the user is who they say they are). (b) Authorization (The process used to decide if the authenticated person is allowed to access specific information or functions) and(c) Access Control (Restriction of access-includes authentication & authorization). Mostly user select password that is predictable. This include both graphical and text based passwords. Users trends to memorable password, unfortunately it means that the passwords tend to follow predictable patterns that are easier for attackers to guess. If the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. various graphical password systems has been developed; Study shows that text-based passwords suffer with both security and usability problems. Based on a recent news article, a security team at a company ran a network password cracker and within 30 seconds and they identified about 80% of the passwords.

A. Purpose

Usable security has unique usability challenges because the need for security often means that standard human-computer-interaction approaches cannot be directly applied. An important usability goal for authentication systems is to support users in selecting better passwords.

Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. So researchers of modern days have gone for alternative methods wherein graphical pictures are used as passwords.

Graphical passwords essentially use images or representation of images as passwords. Human brain is good in remembering picture than textual character. There are various graphical password schemes or graphical password software in the market. However, very little research has been done to analyze graphical passwords that are still immature.

There for, this project work merges persuasive sequence of juncture images and password guessing resistant protocol. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. Well known security threats like brute force attacks and dictionary attacks can be successfully abolished using this method.

II. Security Analysis

A. PASSMATRIX

The security weakness of the traditional PIN method, (2) the easiness of obtaining passwords by observers in public, and (3) the compatibility issues to devices, we introduced a graphical authentication system called PassMatrix. In PassMatrix, 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. Figure 5 demonstrates the proposed scheme, in which the first pass-square is located at (4, 8) in the first image, the second pass-square is on the top of the smoke in the second image at (7, 2), and the last pass-square is at (7, 10) in the third image. In PassMatrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the PassPoints [7] scheme. Based on the user study of sequence of juncture image method does a good job in helping users recollect and remember their passwords. If the user clicks on an incorrect region within the image, a different image will be shown to give the user a warning feedback. However, aiming at alleviating shoulder surfing attacks, we do not recommend this approach since the feedback that is given to users might also be obtained by attackers. Due to the fact that people do not register a new account or set up a new screen lock frequently.

III. Proposed Model

In the proposed model we have integrated sound signature to help in recalling the password. No system has been devolved so far which uses sound signature in graphical password authentication. Study says that sound signature or tone can be used to recall facts like images, text etc. In daily life we see various examples of recalling an object by the sound related to that object enters User ID and select one

sound frequency which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Profile vector is created.

A. *Profile Vectors-*

The proposed system creates user profile as follows-

Master vector - (User ID, Sound Signature frequency, Tolerance)

Detailed Vector - (Image, Click Points)

As an example of vectors -

Master vector (Smith, 2689, 50)

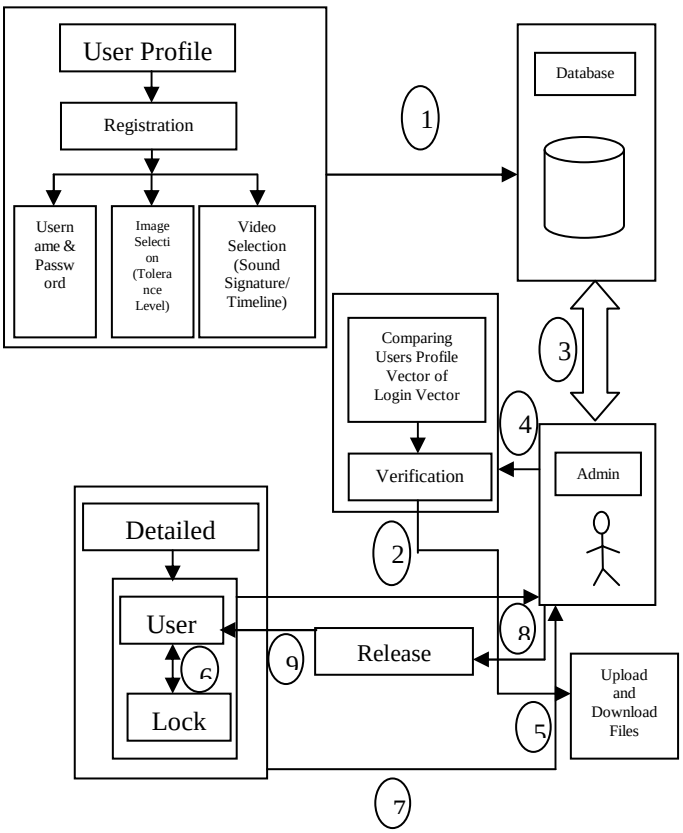
Detailed Vector

Image	Click points
I 1	(128,678)
I 2	(176,134)
I 3	(450,297)
I 4	(760,164)

B. *Advantages:*

1. No system has been devolved so far which uses sound signature in graphical password authentication.
2. To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice.

IV. SYSTEM ARCHITECTURE



V. SYSTEM MODULES

Create User Profile Vector (Master Vector):
Create Detailed Vector (Login Vector):
Compare User Profile/Login Vector:
Upload/Download Module:
Embed the Data:
Extract the Data:

A. *Create User Profile Vector (Master Vector):*

While registration of user information, the user id, sound frequency or time and tolerance are getting for creating master vector.

Master vector – (User ID, Sound Signature frequency, Tolerance)

B. *Create Detailed Vector (Login Vector):*

To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Then Detailed vector is created.

Detailed Vector - (Image, Click Points)

C. *Compare User Profile/Login Vector:*

Enters User ID and select one sound frequency or time which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. Users preferred sequence of juncture images to Pass Points, saying that selecting and remembering only one point per image and sound signature helps considerably for login.

D. *Upload/Download Module:*

Admin are going to upload secret file between them. They can share the uploaded files. User (Military) uses sound signature for download files. System showed very good Performance in terms of speed, accuracy, and ease of use.

E. *Embed the Data:*

Data embedding has direct applications in data mining, data indexing and searching, information retrieval, and multimedia data processing. As two representative techniques for data embedding, both Isomap and Locally Linear Embedding (LLE) require the construction of neighborhood graphs on which every point is connected to its neighbors. This paper reviews several techniques that have been developed to construct connected neighborhood graphs. These methods have made Isomap and LLE applicable to a wide range of data including under-sampled data and non-uniformly distributed data.

F. *Extract the Data:*

Surprisingly, Illustrator does not allow you to extract embedded images. Once embedded, you cannot convert the files back to linked unless you have the original files. You may pick the images one by one and export artwork to a suitable image format, like Photoshop Document (PSD) or Tagged Image File Format (TIFF). But when you try to relink the exported images instead of the original ones, problems arise. The embedded images could be rotates, scaled or

Notes

1. User Normal Login

simply have a different resolution. And, what is really important for print production, spot colors are lost upon export.

VI. CONCLUSION

Here, I kindly convey that special feature of this software is the geniality and it can be worded on the personal computer, since the web page gives a variety option and the message gives clear understanding of the next page it is easy to follow and use.

We have proposed a novel approach which uses sound signature to recall graphical password click points. No previously developed system used this approach. This system is helpful when user is logging after a long time. In future systems other patterns may be used for recalling purpose like touch of smells, study shows that these patterns are very useful in recalling the associated objects like images or text.

REFERENCES

[1] M. Martinez-Diaz, J. Fierrez, and J. Galbally, “Graphical passwordbased user authentication with free-form doodles,” IEEE Transactions on HumanMachine Systems, vol. PP, no. 99, pp. 1–8, 2015.

[2] S. Gurav, L. Gawade, P. Rane, and N. Khochare, “Graphical password authentication: Cloud securing scheme,” in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.

[3] T. Kwon, S. Shin, and S. Na, “Covert attentional shoulder surfing: Human adversaries are more powerful than expected,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6, pp. 716–727, June 2014.

[4] De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. Smith, “Now you see me, now you don’t: Protecting smartphone authentication from shoulder surfers,” in Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems, ser. CHI ’14. New York, NY, USA: ACM, 2014, pp. 2937–2946.

[5] M. Martinez-Diaz, J. Fierrez, and J. Galbally, “The doodb graphical password database: Data analysis and benchmark results,” Access, IEEE, vol. 1, pp. 596–605, 2013.

[6] Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, “The pone lock: Audio and haptic shoulder-surfing resistant pin entry methods for mobile devices,” in Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser. TEI ’11. New York, NY, USA: ACM, 2011, pp. 197–200.

[7] Birget, J.C., D. Hong, and N. Memon. “Graphical Passwords Based on Robust Discretization”. IEEE Trans. Info. Forensics and Security, 1(3), September 2006.

[8] Blonder, G.E. “Graphical Passwords”. United States Patent 5,559,961, 1996.

[9] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. “A Second Look at the Usability of Click-based Graphical Passwords”. ACM SOUPS, 2014.

[10] Cranor, L.F., S. Garfinkel. “Security and Usability”. O’Reilly Media, 2005.

[11] Davis, D., F. Monrose, and M.K. Reiter. “On User Choice in Graphical Password Schemes”. 13th SENIX Security Symposium, 2004.

[12] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.

[13] Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security", in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

[14] D. Weinshall and S. Kirkpatrick, "Passwords You’ll Never Forget, but Can’t Recall", in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.