ISSN:0975-9646

Enhanced Security Layer by Using Integration of Sound Signature and Graphical Password Authentication System

Manasa Bhat[1], Vanisha PSanthmayor[2], Mahesh .K [3]

[1,2]PG Student, Dept. of CSE, AIET ,Moodbidri,India

[3]Asst. Prof , Dept.of CSE, AIET,Manipal ,India

Abstract— Password is used for authentication purpose and it is used to identify the user in computer or any other communication system. Graphical password involves the clicking and dragging activity on the image and integration of sound signature provides addition layer of security. In text based password it is difficult to remember the harder password and if we use easier password then it is easy to guess and also key space is limited. According to psychology human can remember easily images or pictures than texts. Integration of sound signature and graphical password provides better security and also cued click point is used here. If the click point is within the tolerance region and pause time of the audio is proper then password is accepted and user is authenticated.

Index terms- CCP, Tolerance, Sound signature, Authentication, GPAS

I. INTRODUCTION

Human factors are usually thought-about the weakest link in an exceedingly pc security system. There are 3 major areas where the human pc interaction is important: authentication, security operations, and developing secure systems. User authentication is that the most important component within the field of Information Security. For the majority of pc systems, passwords are the tactic of selection for authenticating users. Authentication is that the initiative of knowledge security. Authentication refers to the method of confirming or denying individual's claimed identity. Authentication schemes need users to remember the passwords and recall them throughout log-in time. Mostly users choose positive identification that's sure. This happens with each graphical and text based passwords.

Users tend to decide on unforgettable positive identification, sadly it means the passwords tend to follow sure patterns that area unit easier for attackers to guess. Whereas the certainty drawback will be solve by disallowing user selection and assignment passwords to users, this typically ends up in usability problems since users cannot simply bear in mind such random passwords.

The primary goal of the present user authentication technology is to create the secure nevertheless easier for the user. Graphical password authentication systems (GPAS), that comprises clicking or dragging activities on the image or picture instead of typewriting characters, can be the choice to beat the problems that arise from the text-based positive identification system.

Graphical password authentication schemes are different than text-based schemes, impelled notably by the very fact that humans will bear in mind pictures higher than text. Psychological studies have shown that individuals will bear in mind pictures higher than text. Images are typically easier to be remembered or recognized than text, particularly images; those are easier to be remembered than random pictures.

It's conjointly been steered that graphical passwords could also be laborious to guess or broken by brute force search. If the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer better resistance to dictionary attacks. Because of these benefits, there's a growing interest in graphical password authentication. Additionally to digital computer and internet log-in applications, graphical passwords have conjointly been applied to ATM machines and mobile devices.

GPAS is an authentication mechanism that supports usability and security. Cued click points (CCP) is a click-based graphical password authentication scheme which comes under a cued-recall graphical password authentication technique. Additionally user is asked to pick out a sound signature during the registration process. Varied GPAS are planned as alternatives to text based passwords. It will be used as password authentication for folder lock, web-driven applications, desktop lock etc.

II. RELATED WORK

Text based password is the one which has secret word or string of characters to identify the user in computer or any other communication system. Text based passwords are vulnerable to attack. In the existing system, Brostoff along with Sasse carried out an empirical study of passfaces [5], which illustrates a graphical password recognition system which is shown in the Fig 1. In Passface scheme user has to click on faces to create password. Blonder-style passwords support cued recall method. A user clicks on many antecedently chosen locations in a very single image to log in. As enforced by Passlogix Corporation, the user chooses many predefined regions in a picture as his or her password. To log in, the user should click on selected regions in the image.

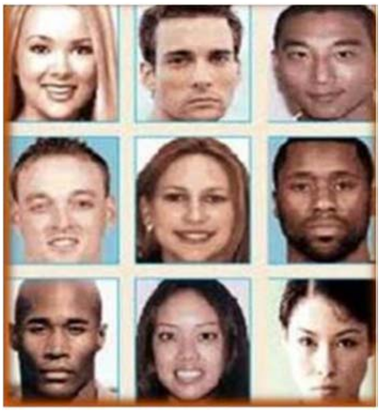

Fig 1: Passface scheme

In Triangular scheme [5][8], we have to select the object from the single image in triangular fashion like first click, second click and third click which is shown in the Fig 2 as password. If those clicks are proper then only the user's password is authenticated. In triangular scheme it is difficult to get an image which has many objects in the single image.

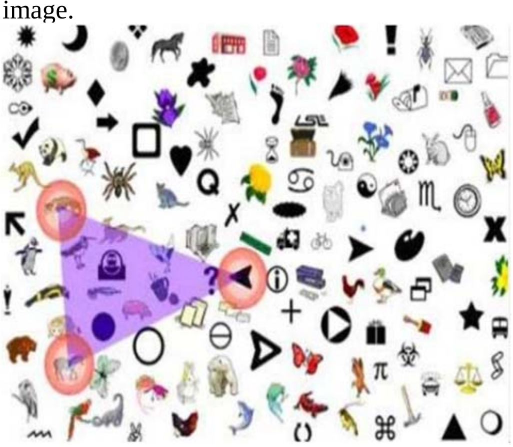

Fig 2: Triangle scheme

In Passpoint scheme [2], we can click anywhere in the image to create the password. Here we have to remember the sequence and it is suitable for the image which contains lot of object. That is Passpoint scheme is best suited for cartoon like image. Cued click points is an alternative to Passpoint scheme. In Cued click-points, user clicks one point on every five pictures instead of on 5 points on one image. It offers cued-recall. Every click leads to showing a next-image, in result leading users down a "path" as they click on their sequence of points. A wrong click leads down incorrect path, with a precise indication of authentication failure solely when the ultimate click. Range of graphical watchword systems has been developed. Study shows that text-based passwords suffer with each security and usefulness issues.

III. DRAWBACKS

Although PassPoints is relatively usable, security weaknesses make passwords easier for attackers to predict. It seems obvious that some areas of an image are more attractive to users as click-points. Hotspots are areas of the image that have higher likelihood of being selected by users as password click-points. If this phenomenon is too strong, the likelihood that attackers can guess a password significantly increases. If attackers learn which images are being used, they can select a set of likely hotspots through image processing tools or by observing a small set of users on the target image and then building an attack dictionary based on those points. Attackers who gain knowledge of these hotspots through harvesting sample passwords can more successfully guess PassPoints passwords. Users also tend to select their click-points in predictable patterns, which can also be exploited by attackers even without knowledge of the background image; indeed, purely automated attacks against PassPoints based on image processing techniques and spatial patterns are a threat.

IV. PROPOSED SYSTEM

A password authentication system must support the strong passwords and it must easy to remember. It's planned that authentication schemes permit user selection whereas influencing users toward stronger passwords. The task of choosing strong passwords is difficult in text based password. This approach makes selecting a safer password the trail of least effort. Instead of increasing the burden on users, it's easier to follow the system's suggestions for a secure password – a feature lacking in most schemes. This approach is applied to make the primary persuasive click-based graphical password system. Here wrong click leads to the different image as shown in Fig 3 with green arrow. At the end password is not authenticated. Correct click on the image within the tolerance region follows the correct image as shown in Fig 3 with black arrow. So password is authenticated if the click is within the tolerance region of the image.

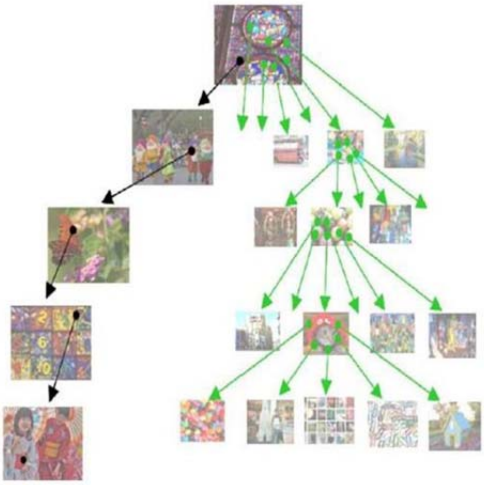

Fig: 3 Each click point in the same image leads to different next image

In addition a sound signature is integrated to help recalling the password. No system has been devolved that uses sound signature in graphical password authentication scheme. Study says that sound signature or tones are often accustomed recall facts like pictures, text. During the registration time audio must be selected and pause time is determined then it is encrypted and stored in the database.

Later while lock or unlocking the folder if the click points are proper then audio will be played and that audio is paused then encryption of that video is done. It is compared with database if it is matched then next image is displayed.CCP is that the best graphical password authentication technique

Fig 4 indicates how to lock and unlock the folder. To lock and unlock folder combination of sound signature and graphical password is helpful. It enhances the security. First we have to select the image from the system or own created. Next audio must be selected and pause time for that audio is selected. Picture selection process and sound selection combined to create the password. These processes are used to lock and unlock the folder.

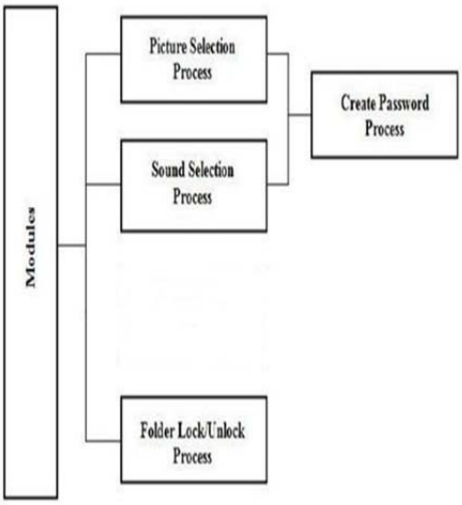

Fig: 4 Folder Lock/Unlock

V. Advantages Of Proposed System

This system is easy for people to use because it involves clicking on the image and pausing of the audio. It provides better security because here graphical password as well as sound signature is used. Key space is large in this system. This system provides the memorability, according to the psychology it is easy to remember the picture and audio rather than the text.

VI. Conclusion

The general goal is to enhance the security by using the combination of sound signature and graphical password authentication system. This method shows usable and unforgettable authentication mechanism. By taking advantage of users' ability to acknowledge pictures and also the memory trigger related to remember the click point and pause time, CCP has benefits over PassPoints in terms of usability. Being cued as every pictures shown associate degreed having to recollect onlyone clickpoint per image seems easier than having to recollect a measure of clicks on one image. Additionally the sound signature helps the user to remember the sequence of the image. CCP offers a safer mechanism compared to PassPoints. CCP will increase the work for attackers by forcing them to initial acquire image sets for every user, so difficult to conduct hotspot analysis on each of those pictures.

References

[1] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. "PassPoints: Design and evaluation of a graphical password system", *International Journal of Human Computer Studies*, 2013.

[2] Arash Habibi Lashkari, Abdullah Gani, Leila Ghasemi Sabet and Samaneh Farmand," A new algorithm on Graphical User Authentication (GUA) based on multi-line grids", ISSN 1992-2248 ©2010 Academic Journals

[3] K. Renaud. "On user involvement in production of images used in visual authentication", *Journal of Visual Language and Computing*, 2011.

[4] S. Singh, and G. Agarwal, "*Integration of Sound Signature in Graphical Password Authentication System*", IJCA January 2011.

[5] Farnaz Towhidi, Maslin Masrom "A Survey on Recognition-Based Graphical User Authentication Algorithms", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009

[6] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud. "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems", *International Journal of Human-Computer Studies*, 63(1-2):128-152, 2005.

[7] D. Davis, F. Monrose, and M. Reiter. "On user choice in graphical password schemes", *13th USENIX Security Symposium*.

[8] Julie Thorpe, P.C. van Oorschot. "Towards secure design choices for implementing graphical passwords. Proceedings of the 20th annual computer security applications conference," December 2004 Ottawa, Ont., Canada: 50 – 60.

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

[10] J. Thorpe and P. C. v. Oorschot. "Towards Secure Design Choices for Implementing Graphical Passwords", *20th Annual Computer Security Applications Conference (ACSAC) IEEE*, Tucson, USA

[11] A. P. Sabzevar, A. Stavrou, "*Universal Multifactor authentication system Using Graphical Password"*

[12] P. Golle and D. Wagner. "Cryptanalysis of a cognitive authentication scheme", *IEEE Symposium on Security and Privacy*.

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

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

[15] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based Graphical Passwords. ACM SOUPS, 2007