International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

INCREASE THE REMEMBRANCE OF THE PASSWORD USING GRAPHICAL PASSWORD WITH A SUPPORT OF SOUND SIGNATURE

Suvarnalata Hiremath, Asst.Prof BKEC, Suvarna2084@yahoo.com
Gangadhara G H, Asst.Prof BKEC, gangadhara_h@yahoo.com
Akash Vastrad, Asst.Prof MSBECL, akashvastrad@gmail.com
Gururaj R. Patwari, Asst.Prof BKEC, gr.patwari26@gmail.com

***Abstract* - It's a new technology which has continued to provide cost-effective, high quality security solutions, tailored to protect our client's products and documents against counterfeiting and fraud. Graphical authentication is proposed to be the alternate for textual passwords since it could be simple for users to remember. Here a graphical password system with a supportive sound signature to increase the remembrance of the password is discussed. In proposed work a Select based graphical password scheme called Phonemes Select Points (PSP) is presented. In this system a password consists of collection 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 each click point this sound signature will be used to help the user in recalling the click point on an image. We propose to extend our existing work for supporting sound signature process for higher authentications in integrating security of data for accessing service. Our experimental results show efficient data security in login process authenticated by the other users.**

KEYWORDS:
Sound Signature, Image Authentication, Recognition, Recall, Cued recall, Human Factors, Graphical Passwords, Tolerance

I.INTRODUCTION

Users employ passwords as a kind of authentication to properly identify themselves on any computer or communications network. Graphical passwords provide one such substitute for traditional passwords approaches. The essential premise is pictures are much easier to remember or recognize than text. Many different schemes could have been proposed for users to utilize pictures or drawings instead of entering text characters [2-7].The predictability problem can be solved by disallowing user choice and assigning passwords for people, this usually gets to usability issues since users cannot easily remember such random passwords. Image Authentication- Establishes that the user is who they say they are. Authorization- The process used to decide if the authenticated person is allowed to access specific information or functions. Access Controls-Restriction of access-includes authentication & authorization. Mostly user select password that is predictable. This happens with both graphical and text based passwords. Users tend to choose memorable password, unfortunately it means that the passwords tend to follow predictable patterns that are easier for attackers to guess. While 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. Number of graphical password systems has been developed; Study shows that text-based passwords suffer with both security and usability problems.
According to 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. It is well know that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human characteristic.

II. RELATED WORK

A. Password problems

The password problem arises largely from limitations of humans' long-term memory (LTM). Once a password has been chosen and learned the user must be able to recall it to log in. But, people regularly forget their passwords. If a password is not used frequently it will be even more susceptible to forgetting. A further complication is that users have many passwords for computers, networks, and web sites. The large number of passwords increases interference and is likely to lead to forgetting or confusing passwords. Users typically cope with the password problem by decreasing their memory load at the expense of security. Another problem of this system is the need for the predefined regions to be readily identifiable. In effect, this requires artificial, cartoon-like images rather than complex, real-world scenes.

B. Why we use graphical passwords?

In a graphical password system, a user needs to choose memorable locations in an image, and at retrieval time users will be presented with either a recognition task or a cued recall task. Here the user has to be able only to recognize previously seen images, making a binary choice of whether the image is known or not known. Recognition is an easier memory task than pure, unaided recall. In this system we use an intermediary form of recollection between pure recall and

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

recognition, cued recall.Graphical passwords have been classified into three basic categories based on their remembrance viz: Recognition, Recall and Cued Recall. Considerable work has been done in this area, the best known of these systems are Passfaces. Brostoff and Sasse (2000) carried out an empirical study of Passfaces, which illustrates well how a graphical password recognition system typically operates. Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in. As implemented by Passlogix Corporation (Boroditsky, 2002), the user chooses several predefined regions in an image as his or her password. To log in the user has to click on the same regions the problem with this scheme

III. PROPOSED SYSTEM MODEL

A password authentication system should encourage strong passwords while maintaining memorability. It is easier to follow the system's suggestions for a secure password a feature lacking in most schemes rather than increasing the burden on users.An authentication schemes allow user choice while influencing user's towards stronger passwords. In this system, the task of selecting weak passwords (which are easy for attackers to predict) is more tedious, discouraging users from making such choices. In the proposed work along with graphical password, sound signature has been integrated to help recalling password. No system has been devolved so far which uses sound signature and graphical password authentication. Study says that sound signature or tone can be used to add facts like images, text etc. Our idea is inspired by this novel human ability. Research says that human can remember images as well as sound tone easily; by applying this method we design our project so it will provide more security. Observed that all student who were registered entered their graphical password and video sound clip and it will be more secured from their point of view it is very good for Graphical and sound clip password authentication system.

IV. SYSTEM ARCHITECTURE

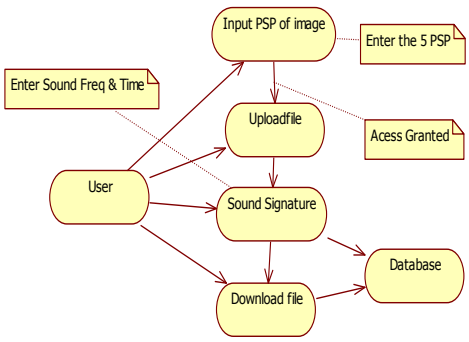


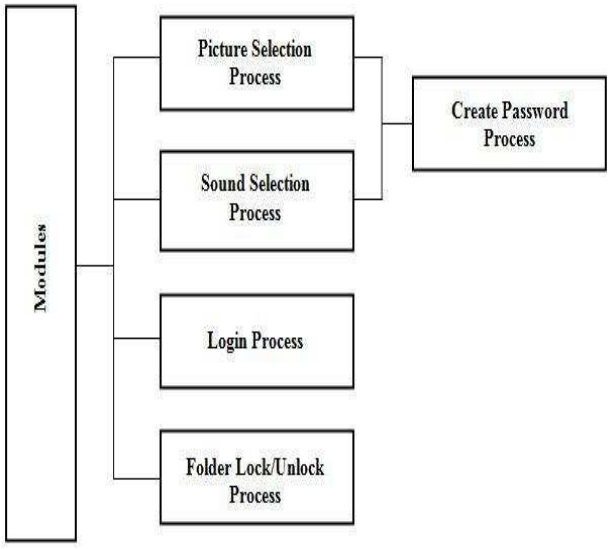
Fig1: Proposed System Architecture

Fig1: Incipient working: Firstly we need to enter the PSP of image. If entered PSP's are correct then system will allows user for next level of logging. In next level user required to enter the volume level, if volume level is correct system will allows for next authentication level. In last stage of logging user need to enter correct video timing. If any of them (PSP's, Volume level, Video timing) are incorrect then system will go in halt state for next 12 hours. After completion of 12 hours reboot again and user can try for uploading and downloading of data by entering correct password for all stages.

System Implementation

The implementation has mainly three modules:

1) Create Password Module
2) Login Module
3) Verification Module
4) Folder Lock/Unlock Module



Create Password Module: User is asked to select the tolerance dimension during password creation. In addition user is asked to select a sound signature or music which helps the user in order to remember the click-points during login phase even if the user tries to login after a long time. Login Module: In login module, the user can give their username and password. In addition, a sound signature is integrated to help in recalling the password. Hacking of username and password can be done. But if the pixels are pointed out correctly, then only one can login in to user page. During login, if the pixels are clicked correctly, then the selected sound is started to play. Else any other sound will be played. Here number of login attempts is limited to three since an extra protection is essential to our passwordprotected system. Security is the main reason to restrict access. Verification Module: During verification phase, the details that the user enters during registration phase

and login phase are verified. Folder Lock/Unlock Module: Protecting your data and information from certain unwanted and prying eyes may become a dilemma if you end up with enough personal and private data on your computer or on your external storage devices. If it is personal or confidential, it needs protection! Folder lock uses GPAS for protecting your files.

V. EXPERIMENTAL RESULTS

Data collected from 10 participants. Each participant was asked to register himself/herself and then each was invited to for login trail 5 times as legitimate user and 5 times as impostor randomly. Participants were final year engineering students of age group 20-24 Year. According to our survey we got instantaneous positive feedback and response.

VI. CONCLUSION AND FUTURE WORK

We have proposed a novel approach which uses sound signature and graphical password click points. Previously developed system never used this approach this system is helpful when user is logging after every single cycle. In future systems other patterns may be used for security purpose like touch of smells, video graphical click point, study shows that these patterns are very useful in secure login the associated objects like images, text and video clip.

REFERENCES

[1] Birget, J.C., D. Hong, and N. Memon. GraphicalPasswords Based on Robust Discretization. IEEE Trans. Info. Forensics and Security, 1(3), September 2006.
[2] Blonder, G.E. Graphical Passwords. United States Patent 5,559,961, 1996.
[3] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based Graphical Passwords. ACM SOUPS, 2007.
[4] Cranor, L.F., S. Garfinkel. Security and Usability. O'Reilly Media, 2005.
[5] Davis, D., F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes.13th SENIX Security Symposium, 2004.
[6] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.
[7] A. 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.
[8] 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.
[9] Birget, J., Brodskiy, A., Memon, N., Waters, J., Wiedenbeck, S., Authentication using graphical passwords: basic results", *ACM International Conference Proceeding Series*, Vol. 93, 2005
[10] "Authentication using graphical passwords: Effects of tolerance and image choice," in 1st Symposium on Usable Privacy and Security (SOUPS), July 2005.
[11] 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.
[12] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom. "Picture Password: A Visual Login Technique for Mobile Devices," *National Institute of Standards and Technology Interagency Report NISTIR 7030*, 2003.