ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 1, January 2013

Integration of Sound Signature and Graphical Password Authentication System

Suyog S. Nischal[1], Sachin Gaikwad[2], Kunal Singh[3]
Prof. A. Devare[4]

[1,2,3] Student of Dnyanganga College of Engineering And Research, Pune
[4] Professor of Computer Department, ZES's DCOER, Pune

Abstract -

A graphical password system with a supportive sound signature and video clip to enhance the security level in authentication system and it is cued click point based system.

In this system password consist of graphical images in which user can select one cued click-point per image and video clip for authentication. Systems shared very good performance in term of speed, accuracy and enhance the security. User firstly need to specify the enter the ccp's of image, in second step volume level and ternary allowed to play the video for secured login into account. In this system Cued-Click point to users receive immediate implicit feedback as to whether they are on the correct path of logging in. CCP offers both improved usability and security.

***Keywords* – Image Authentication, Sound signature, cued-click point, Video timing.**

I. INTRODUCTION

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 happens with both graphical and text based passwords. Users tend to choose memorable password that are easier for hackers to guess the passwords. Number of graphical password systems has been developed; Study shows that a text-based password tends to lead inadequate security and usability problems. It is well known that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human characteristic that's why in this system combination of ccp's, volume level and video timing. A big necessity to have a strong authentication way is needed to secure all our login accounts as possible, so researches come out with advanced password called graphical password where they trying to improve the password techniques and avoid the weakness of normal password. Based on the two assumptions; first, humans can remember pictures better than alphanumeric characters and second, a picture worth a thousand passwords; some psychological studies and company software seem to agree with these assumptions. As known generally, the main drawbacks for the current graphical password schemes are the shoulder surfing problem and usability problem. Even though graphical passwords are easier to guess and break, but in this system combination of all three types i.e. ccp, volume level and video timing.

II. PREVIOUS WORK

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 is that the number of predefined regions is small, perhaps a few dozens in a picture. The password may have to be up to 12 clicks for adequate security, again tedious for the user. 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. Cued Click Points (CCP) is a proposed alternative to Passpoints. In CCP, users click one point on each of 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on hotspot analysis more challenging. Each click results in showing a next-image, in effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the resulting images, they could create a new password involving different click-points to get different images.

III. PROPOSED WORK

In the proposed work we have integrated sound signature to help with the 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

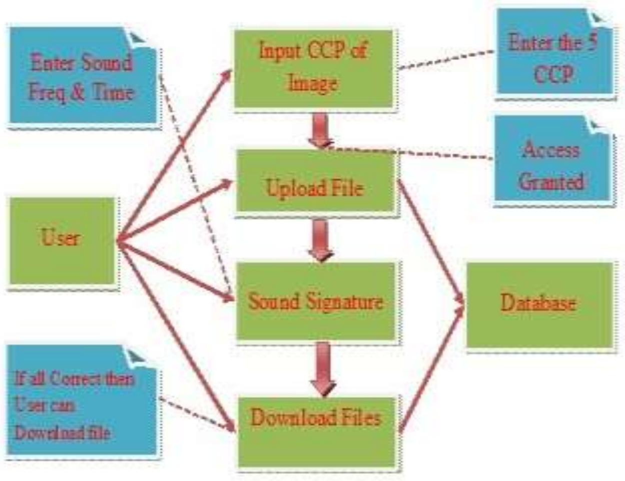

Fig : System Architecture

Incipient working: Firstly we need to enter the CCP of image. If entered CCP'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 (CCP'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.

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

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.

VII. REFERENCE

[1] Pinks, B. and T. Sander. Securing Passwords Against Dictionary Attacks. ACM, CCS, 2002

[2] Thorpe, J. and P.C. van Oorschot. Human-Seeded Attacks and Exploiting Hots-Spots in Graphical Passwords. 16th USENIX Security Symposium, 2007.

[3] van Oorschot, P.C., S. Stubblebine. On Countering Online Dictionary Attacks with Login Histories and Humans-in-the-Loop. ACM Trans. Information and System Security 9(3), 235-258, 2006.

[4] Wiedenbeck, S., J.C. Birget, A. Brodskiy, and N. Memon. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. ACM SOUPS, 2005.

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

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

[7] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based.
[8] Vienna, Austria: ACM, 2004, pp. 1399-1402.

[9]Graphical Passwords. ACM SOUPS, 2007.

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

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

[12] 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.

VIII. AUTHORS

Suyog S. Nischal
Pursuing BE Computer (Final Year).

Kunal Singh
Pursuing BE Computer (Final Year).

Sachin B. Gaikwad
Pursuing BE Computer (Final Year).