Journal of Nonlinear Analysis and Optimization
Vol. 14(3) (2023), March 2023
https://ph03.tci-thaijjo.org/
ISSN : 1906-9685

J.Nonlinear
Anal. Optim

IMPLEMENTATION OF SOUND SIGNATURE IN WEB BASED APPLICATIONS

Dr.R.Shankar
Associate Professor, Department of EEE
Sri Sai Institute of Technology and Science, Rayachoti
Email: shankarr@gmail.com

Abstract:

Many web sites provide login and password as their authentication to their users of that particular web site, sound signature is a new technique for providing authentication for web sites to be accessed in a secured format in these modern period of developing applications that can run on any platform like pc's, Tablet's, or even in Mobiles (Smart phones), here a video clip will be loaded, played while registering and then paused the video clip at certain point time, so this paused point of time can be used as password for that web site to login and also for doing operation present in the web site like uploading, deleting and giving privileges to the users for those applications that are present in our web sites.

Keywords: Authentication System, Sound Signature, Platform.

1. 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).

(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, 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 [1]. 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 [2]. It is well know that the human brain is better at recognizing and recalling images than text [3], graphical passwords exploit this human characteristic.

2. Existing System:

In the existing system**,** Brostoff and sasse 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, 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 in effect, cued click points (ccp) is a proposed alternative to pass points.

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.

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.

3. Proposed System:

In the proposed work 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.

4. CONCLUSION AND FUTURE WORK

We have found 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.

REFERANCES

[1] Saurabh Sing and Gaurav Agarwal, "Integration of Sound Signature in Graphical Password Authentication System", **International Journal of Computer Applications (0975-8887), Volume 12-NO.9, January 2011.**

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

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

[4] Cranor**, L.F., S. Garfinkel**. Security and Usability. O'Reilly Media, 2005.