International Journal of Scientific Engineering and Technology ISSN:2277-1581
Volume No.6 Issue No.5, pp: 164-167 01 May 2017

Code Word Graphical Authentication and Sound Signature

Priyadarshini S., Sharmily.R, Srividhya.G, Vigni Karthika.K
United Institute of Technology
Priyadarshini.cse@uit.ac.in, Sharmily94@gmail.com

***Abstract**: Graphical Password System with a sound signature scheme to increase the remembrance of the password is discussed. The Proposed methodology provides a click based graphical password scheme called Cued Click Points (CCP) is used. In this system, a password consists of a sequence of images in which user can select one click-point per image. In addition, the user is asked to select a sound signature according to click point this sound signature used to help the user to login. The system showed very good Performance in terms of speed, accuracy, and ease of use. Users preferred CCP, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points.*

Keywords: **Graphical Password, Authentication, Sound Signature, Security, Cued Click Points (CCP)**

I. Introduction

There has been a great deal in graphical passwords due to the fact that Primitive's methods suffered from a number of attacks which could be imposed easily. Human factors are often considered the weakest link in a computer security system. To start with most common computer authentication method that makes use of text password. The user natural tendency of the users will always prefer to go for short passwords for ease of remembrance and also lack of awareness about how attackers tend to attack. Unfortunately, these passwords are broken by intruders by several simple means such as masquerading, eavesdropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks. For Blonder, graphical passwords have a predetermined image that the sequence and the tap regions selected are interpreted as the graphical password. Since then, many other graphical password schemes have been proposed. The desirable quality associated with graphical passwords is that psychologically humans can remember graphical far better than text and hence is the best alternative being proposed. There is a rapid interest growing in graphical passwords since they are more or infinite in numbers, thus providing more resistance. Graphical password is more important than text password where the user is asked to remember images or some part of images instead of text or words. 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.

II. Existing Approaches

Existing approaches to Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember.

In the existing system [i] we use text password and graphical password which is easy to remember at the same time easy to crack the password or guess for another user. Also in graphical password, users can recall pictures more than the words. Unfortunately, these passwords are broken by several simple means such as masquerading, eavesdropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks. In Integration of Sound Signature Authentication System 3D [ii] password is constructed by RECOGNITION + RECALL + TOKENS + BIOMETRIC in one authentication system. In Graphical authentication the click points are stored in the database using Message Digest 5 algorithm. The text based passwords are easy to remember so we provide the graphical password, but there are some drawbacks in existing approaches. In Biometrics authentication, the user gives the thumb expression using thumb detection. In sound signature authentication user selects one sound clip and then plays the sound clip pause time is stored in the system database. Identification of sound and particularly human voice has noticeable effect when used as additional biometric data in a system.

In User authentication by secured graphical password [v] implementation implies the graphical password is very strong as compared to text password which is easier to remember. Based on this graphical password technique, the user designed graphical password system is to work as a cued recognition based graphical authentication scheme which allows the user to make images and numbers as user password. The result of the test is very good which indicates that our proposed system early starting is secured.

In Integration Sound Signature Authentication System [iv] the user selects the password which is predictable. This happens with both graphical and text based password user choose a memorable password, unfortunately it means that the password follow predictable pattern which is easier for attackers to guess. Numbers of the graphical password system has been developed. It is well known that the human brain is better at recognizing and recalling images than text. The user proposed the sound signature graphical password includes user chosen the click points in a displayed image. In order to store passwords in the crypto graphical form, we need to prevent small click point from any effect on the password.

Users often create memorable passwords [vii] that are easy

ISSN:2277-1581
01 May 2017

for attackers to guess, but strong system-assigned passwords are difficult for users to remember. Despite the vulnerabilities, it's the user natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance and also lack of awareness about how attackers tend to attacks. Unfortunately, these passwords are broken mercilessly by the unauthorized users by several means such as masquerading, Eaves dropping and other rude means say dictionary attacks, shoulder surfing attack, social engineering attack.

III. Proposed System

The system proposed in multi-layered system to strength security. The system creates the graphical password using a single/multiple images and include sound signature .Password is generated by assigning click points in each image and providing sound above that the SQL server is used to maintain users and provide another security layers. To create graphical password, we need to identify a matrix of images to generate the graphical password and then redirect the images and then password generated for the SQL server database then gives the sound signature to login.

IV. System Architecture

The code authentication system [vi] encourages users to select less predictable passwords, and makes it more difficult where all five click-points are hotspots, specifically, when a user creates a password, user selects click-points within each selected image. The user is also asked to select the tolerance dimension during password creation. In addition, the user is asked to select a sound signature or music which helps the user in order to remember the click-point during log in phase even if the user tries to log in after a long time.

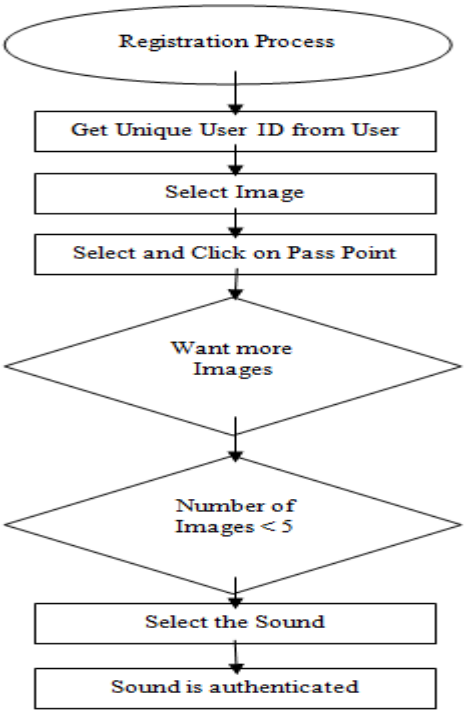

Fig 4.1 System Architecture for Registration Process

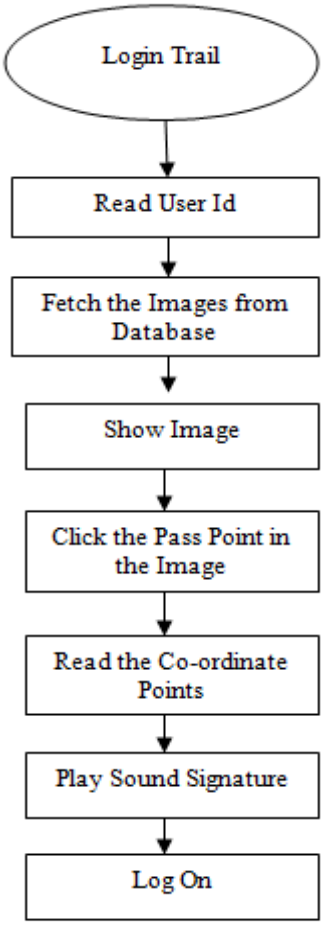

Fig 4.2 System Architecture for Login Process

In login process, 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 managed, but if the pixels are pointed out correctly, then only the user can able to login into the user page. During the login phase, username is taken from the user and it is stored in corresponding variable. If the entered value matches the data in the database which is stored earlier, it will display corresponding user's first image which is selected previously during registration session. And the user can select their previously chosen images by clicking on the specific region or point chosen earlier. After repeating the same steps for all images, comparisons are made. Even if the point chosen in the image was wrong, the user will not be informed about the wrong path which reduces the ability of hacker to guess the password. Else the user is directed to the home page where they can lock or unlock the folders and can also able to change their password as well as the music. During log in, if the pixels are clicked correctly, then the selected sound is started to play. Else any other sound will be played. Here, the number of login attempts is limited to five since an extra protection essential to our password protected system. Security is the main reason to restrict access. Log in attempt limit blocks a user from making future attempts after a

ISSN:2277-1581
01 May 2017

specified limit on retries is reached. During the verification phase, the details that the user enters during the registration phase and login phase are verified.

Fig 4.3 Registration Module

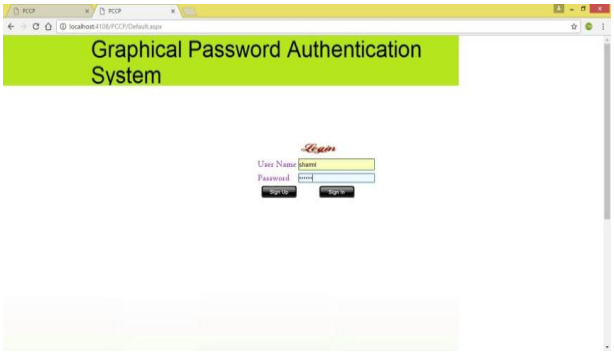

Fig 4.4 Login Module

Fig 4.5 Click Points

Fig 4.6 One Click Point per Image

V. Sound Signature

The analytical report of 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 the User ID and select one sound frequency which he want to be played at login time. The importance of sound signature verification has found and proved its practical applications and significant role in many areas of our life. Example areas of some important key aspects are explosions, screams of people or animal and many other sound-creating events and natural concepts.

To associate sound signature scheme, the users allows choosing an audio file at runtime or using his voice for creating sound file. It strengthens the security of the data. To create detailed vector user asked to select sequence of images and clicks on each image at click points of his choice. Profile vector is created. Enters users ID and select one sound frequency which he wants to be played at login time. To create detailed vector user asked to select sequence of images and clicks on each image at click points of his choice. Profile is created.

The sound signature scheme is used as second level authentication scheme to help the user to login. The system sound signature also has a very good performance in terms of speed, accuracy and ease of use.

In Sound Signature, we have proposed voice recognition to set a next level of authentication. We have used two buttons namely Start and Stop. Once the user clicks the start button it recognizes the user voice which is given as an input and it responds back to the user and produces the output. It connects to the website in which the user has already given in the registration period. It connects to the website. By clicking the stop button the process is terminated.

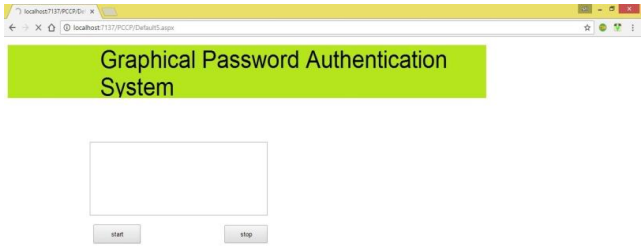

Fig 5.1 Play and Pause Time

VI. Conclusion

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 long time. Voice identification in terms of both speech and speaker authentication has its unique signification and role. 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

i. Birget, J.C, D. Hong, and N. Memon. "Graphical passwords Based on Robust Discretization", IEEE Trans. Info. Forensics and security,1(3).September 2006.

ii. Mr.Jaywant N. Khedkar1, Ms.Pragati P. Katalkar2, Ms.Shalini V. Pathak3, Mrs.Rohini V.Agawane, " Integration of Sound signature in 3D Password Authentication System" , "International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)" Vol. 1, Issue 2, April 2013

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

iv.Blonder "International Journal of Innovative Research in Science & Engineering (IJIRSE)", G.E.Graphical Passwords. United States Patent 5,559,961,1996.

v. Chiasson, S. "Usable Authentication and Click based Graphical passwords." Phd Thesis, Carlton University, Ottawa,Canada. Jan. 2009 .

vi.S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy and N. Memon, "PassPoints: Design and longitudinal valuation of a graphical password system", International Journal of Human-Computer Studies, vol. 63, (2005), pp. 102-127.

vii. D. Weinshall, "Cognitive Authentication Schemes Safe Against Spyware", (Short Paper), IEEE Symposium on Security and Privacy, (2006).