Integration of Sound Signature with Captcha as a Graphical Password

Ms. Aarti Thakur[1] Ms. Apeksha Nagulwar[2] Ms. Swati Jiwatode[3] Ms. Sampada Deshpande[4] Prof. Abhijit Pande[5]

[1,2,3,4,5]Department of Computer Technology

[1,2,3,4,5]RGCER, Nagpur (M.S)

Abstract— Now a day, the graphical passwords are used enormously in order to provide security. Graphical passwords use images as password. Since textual passwords usually suffer from security and usability problem graphical passwords are more acceptable. Graphical passwords are more resistant to intruder attacks and are easy to remember, as humans remember images better than words. In this project we are using Captcha as a graphical password with integration of a sound signature. Captcha is a distorted form of text that must be deciphered during authentication process. The password consists of user-chosen click points in the displayed Captcha. We are integrating the sound signature along with this graphical password to enhance the security of the system. This authentication technique will help in increasing the remembrance of the password and also provide a more secure system.

Key words: Captcha, Graphical password, sound signature

I. INTRODUCTION

The most common computer authentication method is to use alphanumerical usernames and passwords. Passwords are used for – Authentication, Authorization and Access Control. Conventional alphanumeric passwords suffer from disadvantages-they are difficult for the users to remember, particularly if they are arbitrary alphanumeric sequences rather than normal words [6]. Text based passwords are contain string of characters. Users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. Biometric and tokens are used as an alternative to text based passwords but has its own drawbacks such as it requires extra hardware so these methods are costly. As an alternative to all these methods, graphical passwords are used because psychology studied that human brain can recognize images better than the text. Most graphical password systems are based on either recognition or cued recall. In recognition-based systems the user must recognize previously chosen images from a larger group of distracted images [1]. In cued recall password systems users must click on several previously chosen areas in an image. In our project we are using Captcha as a graphical password.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is computer software that prevents intruders from obtaining sensitive information that can protect websites. There are a few different types of Captcha challenge response tests out there such as: text, image, audio and video based Captcha [8]. These different versions have been developed and introduced over the years to aid in preventing 'smarter' intruders passing simpler tests. The various types of Captcha are mentioned below:

- Text based Captcha consist of simple questions those are easy to answer, or show a distorted image of a word.
- Image based Captcha, which are simply visual puzzles.
- Audio based Captcha were developed with the thought of visually impaired users, and it relies on the user listening to the spoken word, and then typing it into a box.
- Video based Captcha will show a video, and then ask for tags which best describe the video.

II. EXISTING METHODOLOGY

In the existing system, Brostoff and sasse carried out an empirical study of pass faces, 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. 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. CCP is the best graphical password authentication technique.

Fig. 1: CCP click-points Scenario

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). 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.

III. RELATED WORK

A. Graphical Passwords:

A large number of graphical password schemes have been proposed. They can be classified into three categories according to the task involved in memorizing and entering passwords: recognition, recall, and cued recall. A recognition-based scheme requires identifying among decoys the visual objects belonging to a password portfolio. A typical scheme is Pass faces wherein a user selects a portfolio of faces from a database in creating a password. During authentication, a panel of candidate faces is presented for the user to select the face belonging to her portfolio. A successful login requires correct selection in each round. The set of images in a panel remains the same between logins, but their locations are permuted. A recall-based scheme requires a user

to regenerate the same interaction result without cueing. In a cued-recall scheme, an external cue is provided to help memorize and enter a password. Pass Points is a widely studied click-based cued-recall scheme wherein a user clicks a sequence of points anywhere on an image in creating a password, and re-clicks the same sequence during authentication. Among the three types, recognition is considered the easiest for human memory whereas pure recall is the hardest.

B. Captcha:

Captcha relies on the gap of capabilities between humans and bots in solving certain hard AI problems. There are two types of visual Captcha: text Captcha and Image-Recognition Captcha (IRC). The former relies on character recognition while the latter relies on recognition of non-character objects. The following principle has been established: text Captcha should rely on the difficulty of character segmentation, which is computationally expensive and combinatorial hard. Machine recognition of non-character objects is far less capable than character recognition. IRCs rely on the difficulty of object identification or classification, possibly combined with the difficulty of object segmentation.

C. Captcha in Authentication:

It was introduced in to use both Captcha and password in a user authentication protocol, which we call Captcha-based Password Authentication (CbPA) protocol, to counter online dictionary attacks. Captcha was also used with recognition-based graphical passwords to address spyware [wherein a text Captcha is displayed below each image; a user locates her own pass-images from decoy images, and enters the characters at specific locations of the Captcha below each pass-image as her password during authentication. These specific locations were selected for each pass-image during password creation as a part of the password..On the contrary, a CaRP is both a Captcha and a graphical password scheme, which are intrinsically combined into a single entity.

The Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of user's ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over Pass Points in terms of usability.

IV. PROPOSED WORK

The proposed system involves integration of sound signature with graphical password. In this project, we will use Captcha as a graphical password. CAPTCHA which is computer software that prevents intruders from obtaining sensitive information that can protect websites. There are a few different types of Captcha challenge response tests out there such as: text, image, audio and video based Captcha. The system intends to create a Captcha based graphical password associated with sound signature. Password is generated by assigning click points in Captcha letter. Associating the sound signature will thereby increase the security of the system and will enhance the performance. The procedure is as follows:
Initially the user will have to login with his/her user id. Then the user will have to click upon the Captcha images and select the perfect click points which the user had clicked while registering itself. Now this clicked pixel value will be matched with the database values. If the value is valid, the next level of security the sound signature phase will be enabled by the system. The user is asked to enter his/her audio as an input. Along with this input the user is also asked to enter the tolerance value in order to determine whether the user is a valid user or an intruder. Even this audio is matched with the database entries. If audio also matches with the previous entries then the system declares the user to be the authenticated user of the system and thereby the user can proceed with the next steps.

If the database values do not match with the entries of the user, the system declares it to be unauthenticated user of the system. And hence the system cannot be accessed by the user. When the next user tries to login into the system this click

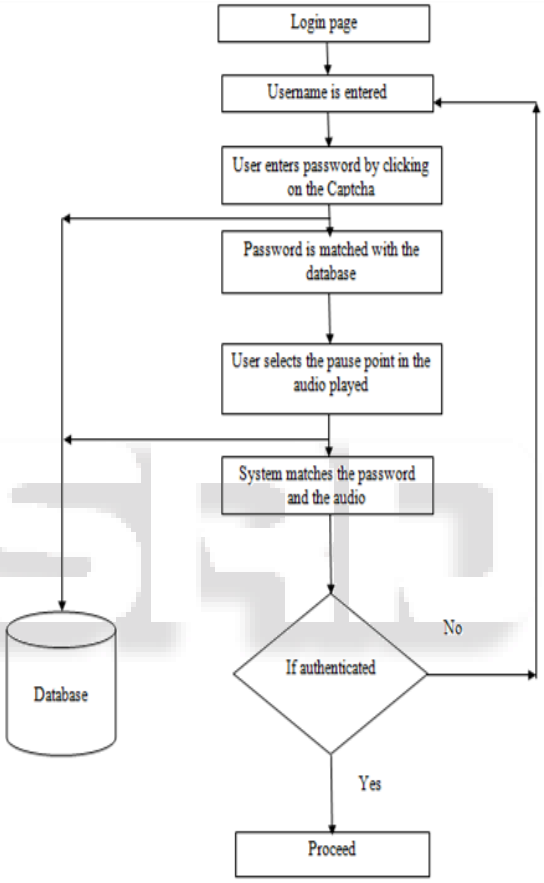


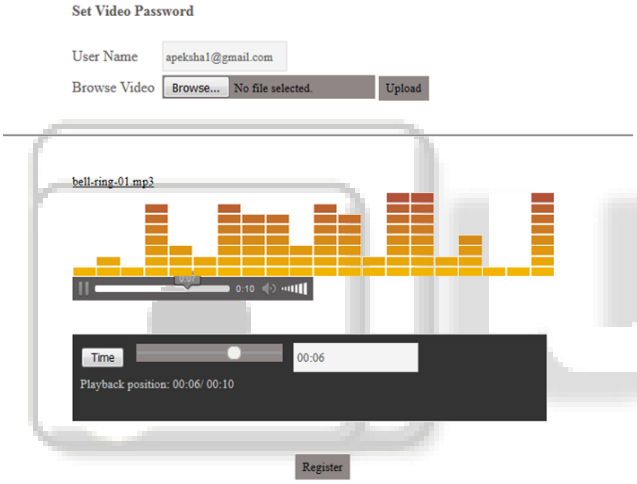
Fig. 2: Working of the System

The figure 3 shows the Captcha as a graphical password. The alphanumeric characters on the graphical image keeps on changing each time a new user will login. The fig.4 shows the Captcha image but with different alphanumeric positions. This will restrict the intruder to guess the password since the positions of the alphanumeric characters keep on changing.

Fig. 3: Graphical Password with Captcha

Fig. 4: Graphical password with changing Captcha

Along with the graphical password we are integrating a sound signature to it. Fig 5 below shows the 2nd phase of registration. Here the user will have to upload a sound file. He/she will have to pause the audio and the timing at which the audio is paused is the next level password for the user. While login phase, the user must pause at the same timing at which he/she had did during registration. If the timings match with the timings that are earlier stored the user is a authenticated user or else the user is unable to access the system resources.



V. Conclusion

We have proposed a novel approach which uses sound signature along with graphical password click points graphical password system with a supportive sound signature is much more helpful as it helps to increase the remembrance of the password. Sound signatures will strengthen the security of the system.

References

[1] Monali D. Supare, Swati V. Badone2, Prof. R.P. Bijwe, "Sound Signature in Graphical Password", International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 3 Issue III, March 2015 IC Value: 13.98 ISSN: 2321-9653.

[2] Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 6, June 2014 891.

[3] Prof. Nitin Ujgare, Abhilasha Deshpande, Sujata Bagade, "Implementation of Integrating Sound Signature with Graphical Password System", International Journal of Computer Trends and Technology (IJCTT) – volume 9 number 1 – Mar 2014.

[4] Ms. Priyanka.S, Ms. Nithya .S, "Captcha as Graphical Passwords with Click Text and Animal Grid Session Password", International Journal of Modern Trends in Engineering and Research, e-ISSN: 2349-9745 @IJMTER-2014

[5] Saurabh Singh, Gaurav Agarwal, "Integration of Sound Signature in Graphical Password Authentication System", 978-1-4121-1951-9/13/$31 © 2013 IEEE.

[6] Bagrudeen Bazeer Ahamed, Shanmugasundaram Hariharan, "Integration of Sound Signature Authentication System", International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012.

[7] Bhusari, "Graphical Authentication Based Techniques", International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013 1 ISSN 2250-3153.

[8] Suyog S. Nischal, Sachin Gaikwad, Kunal Singh, Prof. A. Devare, "Integration of Sound Signature and Graphical Password Authentication System", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 1, January 2013.

[9] Deepasree P O, Avanish Kumar Singh, "Audio Signature in Graphical Password Authentication System", International Journal of scientific research and management (IJSRM) volume 1 issue 4 July 2013.

