ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 16, March 2016

Image And Audio Based Authentication Using Captcha As Graphical Password

R.SARANYA[1] S.USHA[2] ,S.VIGNESWARI[3], M.VIDHYAA[4]
BE Students[1], Asst professor[2]
Department of CSE
P.S.R.RENGASAMY COLLEGE OF ENGINEERING FOR WOMEN

Abstract-- **A new security primitive based on hard AI problems. Network security is the protection of access to files and does not allow hacking by the unauthorized persons. A password consists of one click point per image for a sequence of the image adding sound. A graphical password system with supportive sound signature to increase the remembrance of the password. The next image is displayed is based on the previous click point so user receives immediate implicit feedback and they are on correct path when logging in. It offers both improved usability and security.**

I. INTRODUCTION

Network security consists of policies adopted to prevent unauthorized access. It involves authorization of access to a network,that is controlled by Network administrator. Network security is the variety of computer networks, including public and private Network which conducting transaction and communication among business. Security provides authentication and access control for resources. so, the internet works on implicitly trust one another.

II.PROBLEM STATEMENT

The problem with this scheme is that the number of pre-defined regions is small, a few dozens in a picture user known to choose easily guessable and too short text passwords, which are on easy target of dictionary and brute- force attacks. The username/password is mostly detected by any hackers. This provides data loss in anymanagement system. The goals of this paper is to provide the security for any website using the graphical password with persuasive cued click points.A graphical password system with the supportive sound signature to increase the remembrance of the passwords.In this paper, used the pass point scheme. The composed of several points anywhere on an image. Login attempts that were approximately correct to be accepted

\

III.RELATED WORK

A large number of graphical password schemes have been proposed. They can be classified into three categorized according to the task involved in memorizing and entering the passwords such as recognition, recall, and cued recall.Each type will be briefly described here.More can be found in a recent review of graphical passwords[1]. Captcha relies on recognizing an object by exploiting its surrounding context[1]. Different users may label the same object differently. Captcha relies on recognizing an object by exploiting its surrounding context, a task that humans can perform well .but, it cannot provide full security and authentication. So it can be implemented in future work[1].

A typical scheme is a pass point scheme. [2]Easy for attackers to guess the password because user forms certain patterns in order to remember the secret code which results pattern formation attacks are easily possible. users first choose an ordered sequence of five images and then select the single image to click-draw their secrets. On remaining four images we select click points using features of PCCP (viewport and shuffle button)[2].

The existing work on click-based graphical password schemes using a single background image (e.g., Pass Points) has focused largely on usability. We examine the security of such schemes, including the impact of different background images, and strategies for guessing user passwords[3].

The existing work on click-based graphical password schemes using a single background image (e.g., Pass Points) has focused largely on usability. We examine the security of such schemes, including the impact of different background images, and strategies for guessing user passwords[3].

A recall-base scheme requires a user to generate the same interaction result without cued.Draw-A-secret(DAS)[3] was the first recall based scheme proposed.A user draws her password on a 2D grid.the system encodes the sequence of grid cells along the drawing path as a user-drawn password[3]. In pass point scheme improves DAS's usability by encoding the grid intersection rather than that of the grid cells. Christo Ananth et al. [4] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden.

In a cued-recall scheme, an external scheme is to provide to help memorize and enter a password.pass points [5]scheme is a widely studied the click based cued recall scheme.when the user clicks the sequence of anywhere on an image in creating a password.It is a worth comparing potential password points between text points and traditional click-based graphical passwords such as pass points[5].

IV.PROPOSED WORK

The Ultimate goal of the project work is to provide the security for any websites by using graphical passwords with persuasive cued click-points. A graphical password system with a supportive sound signature. This paper, Captcha as graphical passwords scheme provides high security by using sound for any authentication process. They also offer the approach to address the well-known image in popular graphical password systems, such as Pass Points, that often leads to weak password choices. This paper mainly used for online applications. This threat is widespread and considered as a top Cyber security risk. Defense against online dictionary attacks is a more subtle problem than it might appear.

DIAGRAM

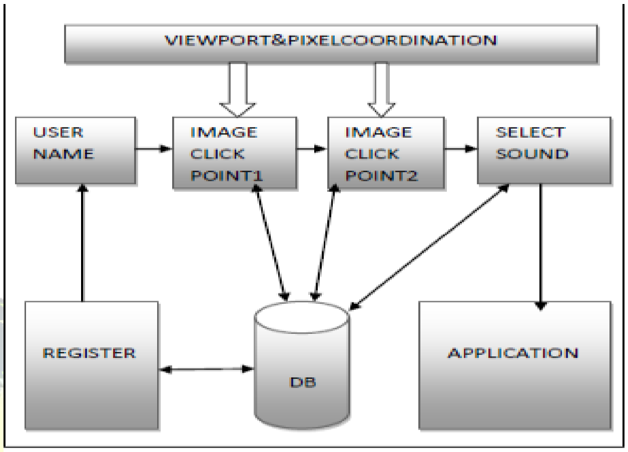

FIGURE1: ARCHITECTURE DIAGRAM

A. *Registration Process:*

The user first creates an individual profile by entering their details. The user and admin can create registration phase using Registration service. Once registered the user can login with their user id and password.

B. *Fixing Tolerance Level:*

The graphical password has a tolerance range that a click by the user choices. Tolerance Level is used for selecting the Co-ordinate pixels in that image.

C. Viewport Selection Mode:

Here, an image has been selected for security purpose. In that image, randomly positioned viewport is used for creating a password.By the Viewport only, the image pixel has been selected.

D. Selecting Pixel Co-Ordination:

In the registration process, to click anyone pixel point in that image only, and the information is stored in the database.

E.Application Maintainance:

A final module of this project application maintenance. That is, to maintain this application with more and more security. Such as username and image click points.

V. PERFORMANCE

“Captcha as a Graphical password a new security primitive based on hard AI problems” is the base paper of this project work. In that, the authors used only images for security purpose.

By using cued click points and random password generation, The sound can be added to an image in particular pixel points.so, it is easy to remember password by the registered candidate and hence, it is high secure.

CONCLUSION

The Ultimate aim of this project is to provide the security for any websites by using graphical passwords with persuasive cued click points. A graphical password system with a supportive sound signature to increase the remembrance of the password.

REFERENCE

[1] Bin B.Zhu, Ning Xu, Jeff Yan, “Captcha as a Graphical Passwords-A New Security Primitive Based On Hard AI Problems”

[2] I.Jermyn, A.Mayer, F.Monrose, M.Reiter, and A.Rubin,”The design and analysis of graphical passwords", in proc.8th USENIX Security., Symp.,1999,pp.1-15.

[3] H.Tao andC.Adams,”pass-go: A proposal to improve the usability of graphicapasswords",Int.J.Netw.Security,vol. 7,no.2,pp.273-292,2008.

[4] Christo Ananth, M.Danya Priyadharshini, “A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks”, International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[5] (2012,feb.).The science Behind Pass faces[online].Available:http://www.real user.com/published/scienceBehindPassfaces. pdf.