Survey on Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems

Prof. T. Arivanantham, Suraj Pratap Deo, Chandan Kumar, Sumit Kumar, Ranjan Kumar

Professor, Dept. of I.T., D.Y.P.I.E.T., Pimpri, Pune, India

Student, Dept. of I.T., D.Y.P.I.E.T., Pimpri, Pune, India

Student, Dept. of I.T., D.Y.P.I.E.T., Pimpri, Pune, India

Student, Dept. of I.T., D.Y.P.I.E.T., Pimpri, Pune, India

Student, Dept. of I.T., D.Y.P.I.E.T., Pimpri, Pune, India

ABSTRACT: We take captcha, an automated test that humans can pass, but current computer programs can't pass any program that has high benefit over a captcha can be used to solve an difficult Artificial Intelligence (AI) problem. Altered Security primitives are based on hard mathematical issue. A CAPTCHA is a computer-based security test used to distinguish human users from unreal users, preventing automated abuse of networked resources. We systematically study the design of image recognition CAPTCHA in this paper. We first understand and examine all IRCs schemes known to us and analyse each scheme against the practical element in CAPTCHA applications, in large-scale real-life applications such as Gmail and Hotmail. CaRP is both a Captcha and a visual protection password plan. CaRP describe a number of protection issues completely, such as on the internet wondering strikes, pass on strikes, and, if along with dual-view technological innovation, shoulder-surfing strikes. Basically, a CaRP protection password can be found only probabilistically by automated on the internet wondering strikes even if the protection password is in the search set.

I. INTRODUCTION

Authentication is a very important task in security where other use text password as A SECURITY TECHNIQUE. BUT TEXT passwords are easy to break by many attacks. Another verification approach for security is alphanumeric password which uses letters, upper case and lower case characters and some certain characters. Today we people use, advanced technologies make use of Graphical Password, CAPTCHA, CaRP for authentication and security purpose. Security provides the most important role in our daily life. For computer system and the information is associated to computer system should also be protected. Different computer system protected using the textual password and the another is biometrics in some system. Idea to provide the security to our computer system or our important data is first of all, give the username and second, give the text password. And new type of password is graphical password. It is the alternative to text password. This threat is widespread and treated as a top cyber security risk. DEFENCE against online dictionary attacks are more subtle problem than it might appear. Automatic counter measures such assmother log on attempts that do not work well for two reasons:

1) It causes the denial-of-service attacks (which were exploited to lock out in the final minutes of eBay auctions and incurs expensive help desk costs for account reactivation.

2) It is not safe to global password attacks where by adversaries aim to break into any account instead a specific one, and thus try each password candidate on multiple accounts and confirm that the number of trials on each account is below the threshold to avoid account lockout.

II.   RELATED WORK

1. Current System:

A large number of graphical password schemes are being proposed. We can classify these into three categories according to the task involved in learning and entering passwords: recognition, recall, and cued recall.

A recall-based scheme requires a user to re-produce the same interaction result without cueing. Draw A Secret was the first recall-based scheme proposed.

2. Proposed System:

In this proposed system, Captcha works on the gap of capabilities between humans and bots in solving some hard AI problems. There can be two types of visible Captcha: text Captcha and Image-Recognition Captcha authentication system for high security.

3. Captcha in Authentication

It was introduced in to use both Captcha and password in a user authentication agreement, which we call Captcha-based Password Authentication protocol, to prevent online dictionary attacks.

The CbPA-protocol in requires solving a Captcha challenge after entering a valid pair of user ID and password unless a valid browser cookie is received.

4. Working

A) Password In The Form Of Graphics

There were varieties of passwords for privacy have been recommended. These all are categorised into three levels based on the privacy and security. An identification based password requires to be remembering for visual basic passwords. The password is encoded by a sequence of grid cells, expressed by two-dimensional coordinate pairs, with "penup" events, rep-resented by distinguished coordinate pairs, added into the place where a pen is lifted from the display surface, or a mouse button is released.

B) Captcha is drawn

The most of the CAPTCHA methods are designed for use on domestic computers or systems. However, many people are using network resources with the help of smaller mobile devices as well as regular computers. The development of a CAPTCHA user verified mechanism suitable for mobile devices is therefore an issue which merits research attention. In particular, the capabilities of smart screens user-interfaces in mobile devices have proven very easy for users.

C) Conversion of Captcha into CaRP

In principle, any visual Captcha scheme relying on identifying two or more predefined types of objects can be converted to a CaRP. All text Captcha schemes and many of IRCs meet such requirements. Those IRCs that rely on identifying a single predefined type of objects can also be changed to CaRPs in general by adding more types of objects. In practice, conversion of a definite Captcha scheme to a CaRP scheme typically requires a case by case study, in order to give assurance both security and usability.

D) Image proposed based on the Captcha

One of advantages of human beings possess over computers is the capacity to identify similar objects within images, in addition of various types of distortion and changes. We used this property of the human visual system for designing a different type of CAPTCHA interface named "CAPTCHA Zoo", intensed especially for mobile devices and especially for young users of present generation of mobile devices.

III.   ARCHITECTURE

The architecture of the proposed system consists of following components:

1. Bank Server:

The Bank server   has following functionalities:

1) To store the details of all merchant servers.
2) To authenticate Merchant server & end user.
3) To generate captcha in 3 level & apply visual cryptography.

2. Merchant Server: A merchant server is an intermediate server which accepts requests from end user and communicates with bank server. The merchant server accepts the share of captcha from Bank sever and sends to end user for authentication.

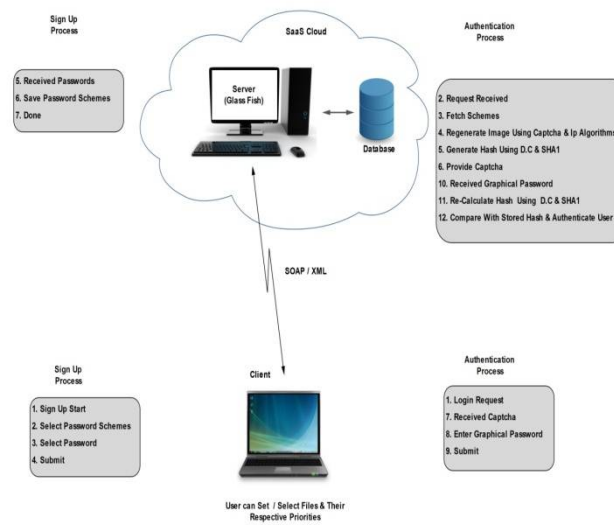The Architecture is shown in following fig1:

Fig1:-captcha password system working Architecture.

3. Client or End User:
Client is the person who is performing the online transactions. It requests merchant server for any transaction and gets response. Client provides its credentials and wait for the captcha from Bank server .It combines the shares from Bank server and Merchant server to get original captcha for further processing.

IV. ALGORITHM

We are using MD5 algorithm with salt. A salt is random data that is used as an additional input to a one way function that hashes a password or passphrase.
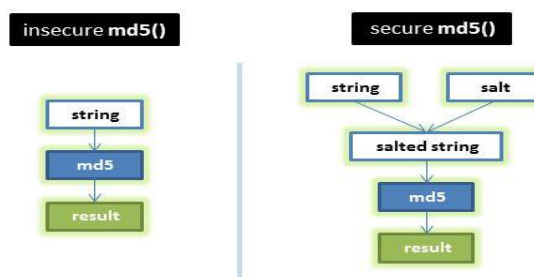

Figure 2: MD5 with Salt

V. APPROACH

The proposed system construct with mainly three different models that are user, server and trusted authority manager as shown in figure 3.
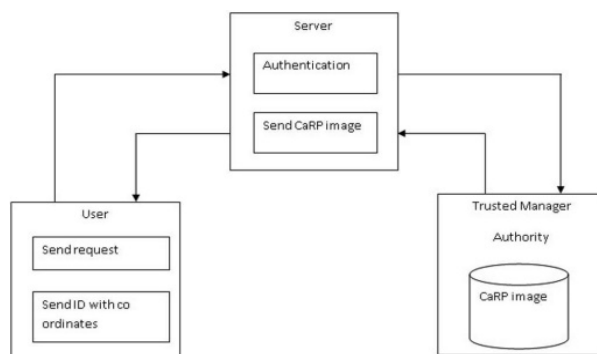
Fig 4: Proposed System

User sends authentication request to the server with visual object IDs or user selects. Server request for the CaRP image through True Authority Manager from the image and sends that image to the user. Server calculates the coordinates sent by the user and login successes if the value matches.

VI.   SUGGESTED METHODOLOGY

Our methodology is based on the Image Captcha validation scheme using visual cryptography. It avoids password and other confidential information from the phishing websites.
The proposed approach can be depending into registration phase:
The phase of registration –

1) The User can add registered login which will be displayed on the home page.
2) Authentication level 1:   The User use any alphanumeric key for level 1 authentication
To his level 1 login password.
3) Authentication level 2:   The User use any images for level 2 authentication to his level 2 login password.
4) Authentication level 3:   The User use any alphanumeric key and special character for level 3 authentication to his level 3 login password.

VII.   CONCLUSION AND FUTURE WORK

In proposed CaRP, a new security primitive depend on unsolved hard AI problems. CaRP is both a Captcha and a graphical password scheme. The clue of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online assuming attacks: a new CaRP image, which is also a Captcha challenge, is used Our proposed technique provides more security as a random image is selected for a particular session and both the encryption and decryption is done with the unique key that is created at the time of user registration. This system provides three level securities and due to use of captcha and Visual Cryptography, the system becomes more secure against the cyber-attacks.

REFERENCES

1. R. Biddle, S. Chiasson , and P. C. van Oorschot , Graphical passwords: study from the first twelve years, ACM Comput.
2. K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, Building segmentation based human-friendly human conection proofs.
3. I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, The design and study of graphical passwords.
4. H. Tao and C. Adams, Pass-Go: A proposal to improve the usability of graphical passwords, Int. J. Netw.
5. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, PassPoints: Design and longitudinal evaluation of a graphical password system, Int. J. HCI, vol.
 6. P. C. van Oorschot and J. Thorpe, On predictive models and userdrawn graphical passwords, ACM Trans. Inf. Syst. Security.
7. N. Joshi. (2009, Nov. 29). Koobface Worm Asks for CAPTCHA [Online].
8. M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage, "Re: CAPTCHAs—Understanding CAPTCHA-Solving.
9. M. Szydlowski, C. Kruegel, and E. Kirda, "Secure input for web applications," in Proc. ACSAC, 2007, pp. 375–384.
10. G. Wolberg, "2-pass mesh warping," in Digital Image Warping.
11. HP TippingPoint DVLabs, New York, NY, USA. (2011). The Mid-Year Top Cyber Security Risks Report [Online].