IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# CAPTHA

*As a New Security Primitive*

[1]Mrs. Snehal Rajole, [2]Mr. Rahul S. Derle
[1]ME Computer Engineering, [2]M. Tech., Computer Science and Engg.,
MVPS's RSM Polytechnic, Nashik, Maharashtra, India

*Abstract:* New space-time authentication techniques are proposed, in this project. In development of authentication techniques,captcha as Graphical Passwords authentication is a new direction .Today's information systems is in a need of obvious identification between communicating entities. The Process of entity identification in general is also called as authentication. The main function of this project is to work on Banking Security.

On hard mathematical problems many security primitives are based . Using the hard AI problems for the sake of security ,it is emerging as an exciting new paradigm, but it has been underexplored. In this project , we have described about a new security primitive which is based on hard AI problems which is a system we call as Captcha as graphical passwords (CaRP) . Captcha and a graphical password scheme both are part of CaRP. A number of security problems , such as online guessing attacks, relay attacks when combined with dual-view technologies, shoulder-surfing attacks is addressed in CaRP

***Keywords* - Graphical password, password, hotspots, CaRP, Captcha, dictionary attack, password guessing attack, security primitive.**

## I. Introduction

Hard mathematical problems dependent on many security primitive. Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. this paper, proposes a new security primitive based on hard AI problems built on top of Captcha technology, which we have given a name called as Captcha as graphical passwords (CaRP).

For the financial world ATMs have brought much relief. By keeping the banking all free of traffic with its attendent issues multiple problems Various problems were solved with the advent of these machines . Work of the bankers became more difficult leading to all forms of errors because of maintaining long queues in the banking hall . Automated teller machines have solved a major problem before bankers close for the days business and have paid comfort to the customers of their homes for financial transactions . The gains of technology brought by this machine to supplement human tellers realized the common man , the joy shall be short lived by various practices leading to financial losses known by little one. As the banks are losing the customers of those banks are also vanishing . As the users are losing money to fraudsters ,media are filled with various forms of complaints. Some people have promised that never to come near the usage of various cards – debit, credit or prepaid – local or international. The problem may lead to a legal battle between banks and their customers . The main focus of this project is to find a long lasting solution.

The system of Current authentication suffer from many weaknesses. As the users do not follow their requirements , Textual passwords are commonly used. As the dictionaries make textual passwords easy to break , Users tend to choose meaningful words from dictionaries. Man available graphical passwords have a password space which is less than or equal to the textual password space. Tokens or Smart cards can be stolen.

CaRP is click-based graphical passwords, to derive a password sequence of clicks on images is used. For an every login attempt a new CaRP image is generated unlike other click-based graphical passwords which is used in CaRP are Captcha challenges. CaRP offers protection against the relay attacks it an increasing threat to bypass Captcha as protection, where Captcha challenges are relayed to solve by the human. If combined with dual-view technologies, CaRP is robust to shoulder-surfing attacks

## II. CAPTCHA

Developed By – Alta Vista (1997) IBM
Standing for "Completely Automated Public Turing Test to tell Computers and Humans Apart". Captcha is Internet security protect online email and other services from being abused by bots.

The two types of Captcha: 1) text Captcha
2) Image-Recognition Captcha (IRC).

A program that are generate and grade tests that:

- Most Human can pass
- Current Computer Program cannot pass

In existing system CAPTCHA is only used to detect human users from bots

## III. GRAPHICAL PASSWORD

Graphical password - authentication system.
That works by having the user select from images in specific order.
Graphical passwords classified into three categories:

1) Recognition-based,
2) Cued-recall,
3) Recall-based.

(Captcha as Graphical Passwords).Click-based graphical passwords is call CaRP. Is generate a sequence of clicks on an image is used to derive a password.

## IV. PARAMETER

Mainly various parameters are used mainly in these three modules they are:

1. User authentication.
2. Image processing.
3. Carp generator

1. User authentication

This module help the CaRP system to authenticate the current user. The user its appropriate login id and go through the set of different carp challenges and it attempts the correct sequence of Graphical password the it become successful logic for the particular user.

Modules are:
1 ) p
2) s
Where,
P= set of password entered by current user.
S= Salt value which stored in data base which contain the correct password store at the time of registrationfor desired User ID.

2. Image processing

This modules is the sub modules of Captcha module in which sequence of image is processed both for registration and for Login process. During image processing various image and the arrangement of their combination is taken in to consideration by using the following sub modules and the parameters:

i. Luminosity contrast.
ii. Color contrast.
iii. Foreground.

3. Carp generator

This parameter used in Carp generators are:

a) CAPTHCHA
b) Graphical password
c) Merging of click image and text points

## V. RELATED WORK

Captcha is used to secure the sensitive user inputs on an untrusted client. This scheme secures the communication channel between user and Web server from key loggers and spyware. The paper did not explore its rich properties and the design space of a variety of CaRP instantiations. Security Analysis of Graphical Passwords over the Alphanumeric Passwords.[2]In this paper, we have conducted a comprehensive study between the alphanumeric and graphical passwords. The main reason for adaption of graphical password is that people are better at memorizing graphical passwords than text-based passwords. CAPTCHA Based Web Security.[3]Usability of Captcha. It is observed that overall usability of CAPTCHA decreases with increase in complexity. Graphical Passwords: Learning from the First Twelve Years.[4]In this paper various Graphical password schemes have been proposed as alternatives to text-based password authentication. Securing Passwords Against Dictionary Attacks.[5]The CbPA-protocol in requires solving a Captcha challenge after inputting a valid pair of user ID and password unless a valid browser received cookies. On Countering Online Dictionary Attacks with Login Histories and Humans-in-the-Loop.[6] An improved CbPA-protocol is proposed in paper by storing cookies only on user-trusted machines and applying a Captcha challenge only when the number of failed login attempts for the account has exceeded a threshold. Limit Online guessing attacks. Revisiting defenses against large-scale online password guessing attacks.[7]Guessing attacks further improved in this by applying a small threshold for failed login attempts from unknown machines but a large threshold for failed attempts from known machines with a previous successful login within a given time frame. Implementing cost is high. A new CAPTCHA interface design for mobile devices.[8]Consequently, this paper proposes a new form of image-based CAPTCHA interface design, well-suited for mobile devices. The design utilizes the convenience of the touch-screen interfaces of mobile devices, and it is intended to be particularly approachable for younger or non-technical mobile device users. Only used for authentication purpose as used in online registration. Understanding CAPTCHA-Solving Services in an Economic Context.[10]This paper includes Study of Estimation Cost of Captcha –solving service for relay attacks. Experimental approach: John the Ripper Password Cracker. [11]This Papers include results of experimental implementation of John the ripper password cracking tool to crack Graphical password(text & click text).

## VI. PROPOSED SYSTEM

The large number of graphical password schemes have been proposed. We present a new security primitive based on hard AI problems, name as, a novel family of graphical password systems built on top of Captcha technology, which we called Captcha as graphical passwords (CaRP).

Module of System:-

1. Registration phase module
2. Login phase module
3. Download file Module
4. OCR Authentication module
5. Captcha Graphical Authentication Module

## VII. ALGORITHM

In real time application there is AS(Authentication server). In our Project we use Secure database as AS.AS contain hash table which contain 2 values p&s as H(P,S).

Where as, P=Entered password.

S(salt)=valid password for particular User.

Algo:

**Step1**:User attempt login request to AS.

**Step2**:AS will receive login request, generate CaRP image by using CaRP generator and also stores the current CaRP image ie sent to the user to click his password

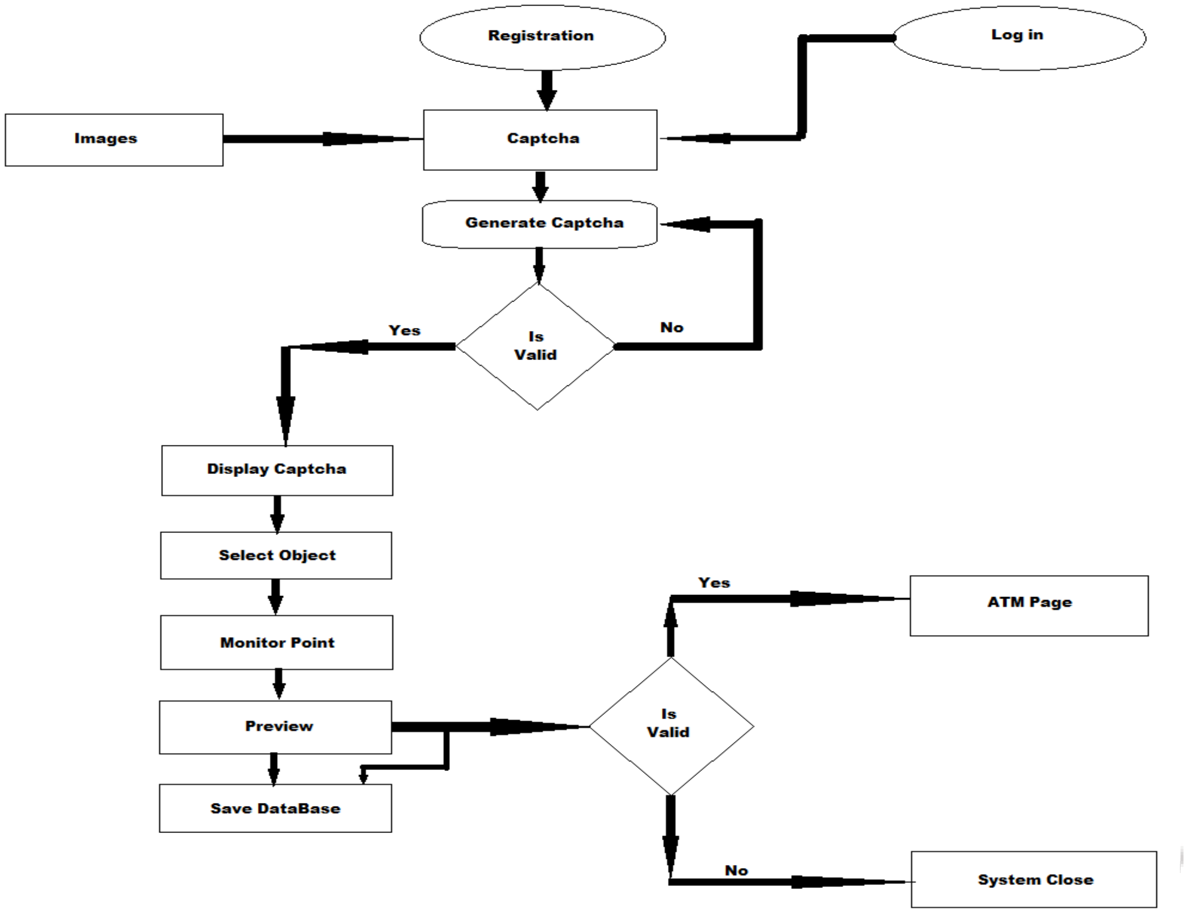
**Step3**:Then User will receive the CARP images and then the user will click the and its text points from the different sets of CaRP images.

**Step4**: The x & y coordinates of clicked points are recorded and sent to AS along with the user ID of that User.

**Step5**:After Receiving the recorded click points, the AS will stores it in the p value of hash table and will retrive the valid password for the User ID from its database and store it in the S value of hash table.

Step6:Login is Successful if P=S.

## VIII. FIGURES / CAPTIONS



## IX. Acknowledgment

we are grateful to the experts those who have contributed towards development of the template and the reviewers for their valuable comments and suggestions.

## References

**[1]** Security Analysis of Graphical password over the Alphanumeric password -G. Agarwal* ( Dec-2010)
**[2]** Overview published Recognition - Sushama Kulkarni* (Nov-2013)
**[3]** R. Biddle, S. Chiasson, and P. C. van Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Comput. Surveys, vol. 44, no. 4, 2012.
**[4]** B. Pinkas and T. Sander, “Securing passwords against dictionary attacks,” in Proc. ACM CCS, 2002, pp. 161–170.
**[5]** P. C. van Oorschot and S. Stubblebine, “On countering online dictionary attacks with login histories and humans-in-the-loop,” ACM Trans. Inf. Syst. Security, vol. 9, no. 3, pp. 235–258, 2006.
**[6]** M. Alsaleh, M. Mannan, and P. C. van Oorschot, “Revisiting defenses against large-scale online password guessing attacks,” IEEE Trans. Dependable Secure Comput., vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.
**[7]** R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, “A new CAPTCHA interface design for mobile devices,” in Proc. 12th Austral. User Inter. Conf., 2011, pp. 3–8.
**[8]** J. Bonneau, “The science of guessing: Analyzing an anonymized corpus of 70 million passwords,” in Proc. IEEE Symp. Security Privacy, Jun. 2012, pp. 20–25.
**[9]** John the Ripper Password Cracker [Online]. Available: http://www. openwall.com/john/
**[10]** Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems.-Bin B. Zhu* (June-2014)