

CAPTCHA as Graphical Passwords A New Security Primitive Based on Hard AI Problems

Ashwini B Gade¹, Shubhangi R. Gunjal¹, Megha D. Jadhav¹, Kamal S Supnar²

Dept. of Computer Engineering SCSCOE, Savitribai phule Pune University Rahuri Factory, Ahmednagar, Maharashtra,
India¹

Assistant Professor, Dept. of Computer Engineering, SCSCOE, Savitribai phule Pune University, Rahuri Factory,
Ahmednagar, Maharashtra, India²

ABSTRACT: In the Network Security, many security primitives are there based on hard mathematical problems. A new paradigm is emerged as an exciting one for the security using hard AI problems. In this paper we present a new security primitive based on hard AI Problems namely CaRP (Captcha as Graphical Passwords). It is a novel family of graphical password systems built on top of captcha technology. It is a graphical password scheme as well as it addresses a number of security problems such as online guessing attacks, relay attacks, and shoulder surfing attacks. A CaRP also offers a novel approach to address the image hotspot problem in popular graphical password systems such as passpoints, that lead to weak password choices. CaRP is not a proper solution but it offers security and us ability for some practical applications for improving online security.

KEYWORDS: Graphical password, CaRP, Captcha

I. INTRODUCTION

Graphical passwords are knowledge-based authentication mechanisms where users enter a shared secret as evidence of their identity. However, where text passwords involve alphanumeric and or special keyboard characters, the idea behind graphical passwords is to leverage human memory for visual information, with the shared secret being related to or composed of images or sketches. Despite the large number of options for authentication, text passwords remain the most common choice for many reasons. Passwords are the most common method of authenticating users, and will most likely continue to be widely used for the foreseeable future, due to their convenience and practicality for service providers and end-users. Although more secure authentication schemes have been suggested in the past. Authentication refers to the process of confirming or denying an individual's claimed identity. Authentication schemes require users to memorize the passwords and recall them during log-in time. Also, adequate authentication is the first line of defense for protecting any resource. Graphical techniques are one of the many alternatives proposed to address the weaknesses in the conventional authentication based upon username and passwords.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), also known as Human Interactive Proof (HIP), is an automated Turing test in which both generation of challenges and grading of responses are performed by computer programs. CAPTCHAs are based on Artificial Intelligence (AI) problems that cannot be solved by current computer programs or bots, but are easily solvable by humans. A client who provides a correct response to a challenge is presumed to be a human. CAPTCHAs have been widely used as a security measure to restrict access from bot. As per Bin B. Zhu present

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

a security analysis of the representative schemes we have identified. For the schemes that remain unbroken, he present our novel attacks. For the schemes for which known attacks are available, he propose a theoretical explanation why those schemes have failed. Next, he provide a simple but novel framework for guiding the design of robust IRCs. Then he propose an innovative IRC called Captcha that is scalable to meet the requirements of large-scale applications. Captcha relies on recognizing an object by exploiting its surrounding context, a task that humans can perform well but computers cannot. Captcha's speed is not a satisfied one, and it does not have large-scale usability.

II. LITERATURE SURVEY

Bin B. Zhu [1] implemented the Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems. This authentication system is based on Animal Grid and Click text which can be used in Smartphone as well as desktop computers.

Hossein Nejati [2] implemented the Deep CAPTCHA: An Image CAPTCHA Based on Depth Perception. In this system 6 images of different objects and different sizes of images is used and user task is to order these images in terms of their relative size.

Hadyn Ellis [3] implemented the Science behind Pass faces. In this system 3x3 grid is used. User also uses the human faces or a numerical keypad value this value is corresponds to the faces on the grid. In that at least 3 to 7 faces user have to select for login process. But in this system required login time can be increased if user selects more pass faces.

P. R. Devale [4] implemented Cued Click Points with Click Draw Based Graphical Password. In this system increasing security using secret drawing in particular image during authentication process. Correct password or incorrect password is displayed after final click.

Pankaja Patil [5] implemented Graphical password authentication using persuasive cued click point. In this system after filling the form user can select user define picture or system define picture after that user have to click any pixels in the images as click point to create graphical password. During creation of password one view port that is randomly positioned on the image User also change this view port if user does not want that view port. View port can be changed using Shuffle. During registration phase user has to click 5 point within that view port and at a login time sequence must be in correct order.

III. SYSTEM ARCHITECTURE

A system architecture is a conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.

Above architecture there are two possibilities that either user is registered or not that means sign in or sign up. If the user is not registered then user has to create an account by giving username and password. And according to that password, user will get a new Captcha challenge every time. By clicking on correct points user can login. Then Authenticated server receives password of particular account and calculate its hash value using algorithm like SHA-1. Authentication is successful if and only if the two hash values are matched.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

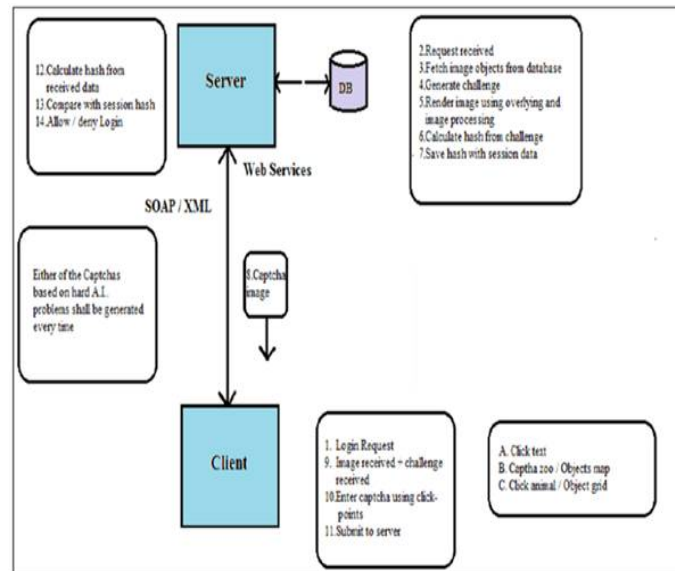


Figure1. System Architecture

IV. METHODOLOGY

A new paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. Is it possible to create any new security primitive based on hard AI problems. This is a challenging and interesting open problem. In this paper, we introduce a new security primitive based on hard AI problems, namely, a novel family of graphical pass-word systems integrating Captcha technology, which we call CaRP(Captcha as graphical Passwords). CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt.

The notion of CaRP is simple but generic. CaRP can have multiple instantiations. In theory, any Captcha scheme relying on multiple object classification can be converted to a CaRP scheme. We present exemplary CaRPs built on both text Captcha and image-recognition Captcha. One of them is a text CaRP wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaRP images. CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. 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. CaRP also offers protection against relay attacks, an increasing threat to bypass Captchas protection, wherein Captcha challenges are relayed to humans to solve. Koobface was a relay attack to bypass Facebook's Captcha in creating new accounts. CaRP is robust to shoulder-surfing attacks if combined with dual-view technologies.

V. EXPERIMENTAL SETUP

In this proposed framework I am making use of Windows Operating System because it is most stable when made a comparison with earlier versions and also because of its networking support. It subsumes remote desktop association which is required in this project and it provides security to code, file and many more that are stored remotely. To

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

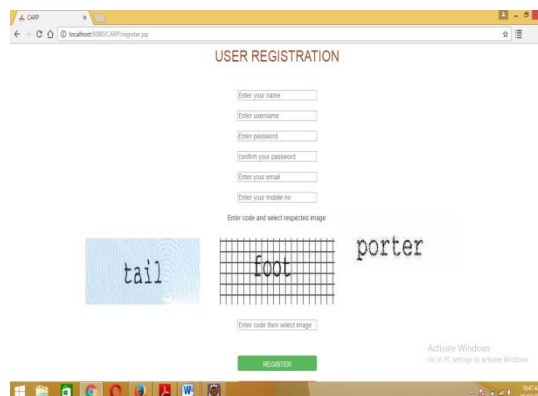
implement the above software framework here “Java Programming” (jdk_1.7) is been used. More precisely Java Server Pages (JSP) is utilized which is a programming language for creating intense, platform self-governing format for constructing Web-Based applications. For the purpose of accumulating the database in this project “MYSQL 5.5” is utilized which offers self-governing platform and also supports the software to work in the entire environment.

VI. IMPLEMENTATION MODULE

The Implemented modules are as follows

- 1) User Registration
- 2) User Sign in
- 3) Administration
- 4) Services

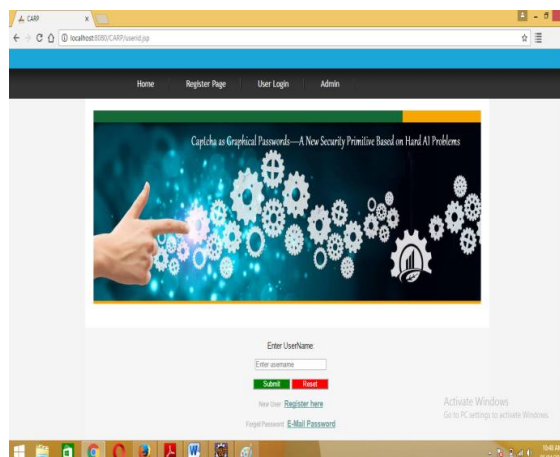
1. User Registration



The screenshot shows a web browser window displaying a "USER REGISTRATION" form. The form includes input fields for "Enter your name", "Enter username", "Enter password", "Confirm your password", "Enter your email", and "Enter your mobile no.". Below these fields is a CAPTCHA section with the text "tail", "foot", and "porter" overlaid on a grid. A "REGISTER" button is located at the bottom of the form. The browser's address bar shows "localhost:8080/CAPT/Registe.jsp".

Fig2. User Registration

2. User Sign in



The screenshot shows a web browser window displaying a "User Sign in" form. The form has a navigation bar with "Home", "Register Page", "User Login", and "Admin" links. The main content area features a banner with the text "Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems" and an image of a hand pointing at a grid of gears. Below the banner is an "Enter Username" input field with a "Submit" button and a "Forgot Password" link. The browser's address bar shows "localhost:8080/CAPT/SignIn.jsp".

Fig3. User Sign in(A)

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

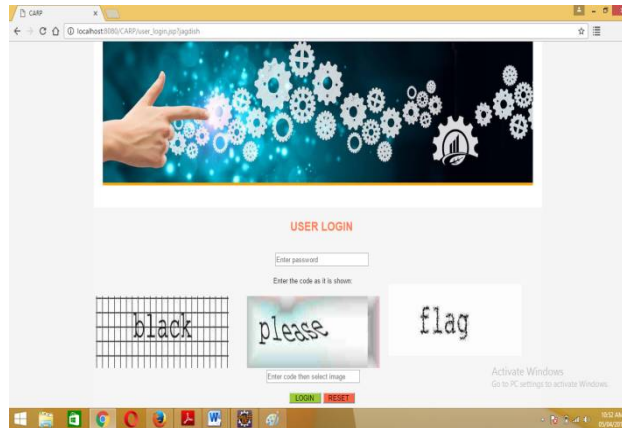


Fig4. User Sign in (B)

1. Administration

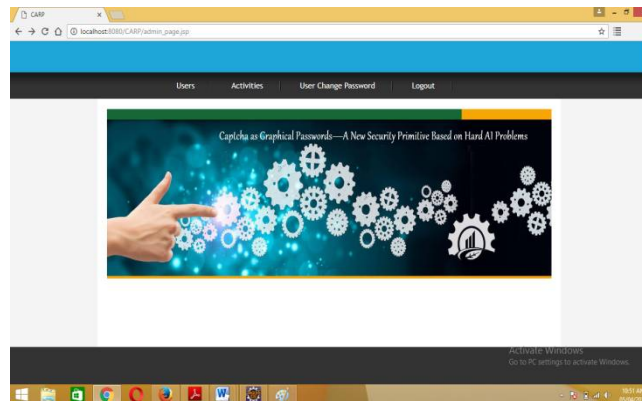


Fig5. Administration

1. Services

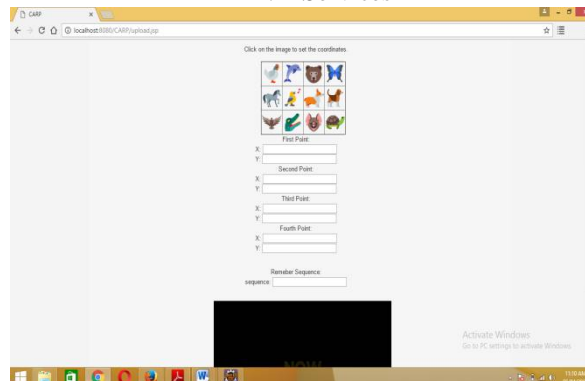


Fig6. Services

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

VII. RESULT ANALYSIS

The following Graph shows the Guessing attack Success Rate on each and every Text and picture captcha password authentication. The result analysis which requires the outcomes of the experimental accepted text and picture password guessing attack success rate for the client's log in sessions We have seen that out of the 100% percent success rates of picture password guessing attacks in animals, flowers, Birds logins are accepted and remaining 95 % and 90 % are in the Fruits and Text logins are accepted and the overall result of Analysis of the guessing success rates are 100 % logins are accepted and remaining 15 % logins are rejected. So red, green and blue portions will provide us the sign in attempted regions completely and light blue and purple portions will provide us the logins are partially accepted ratios.

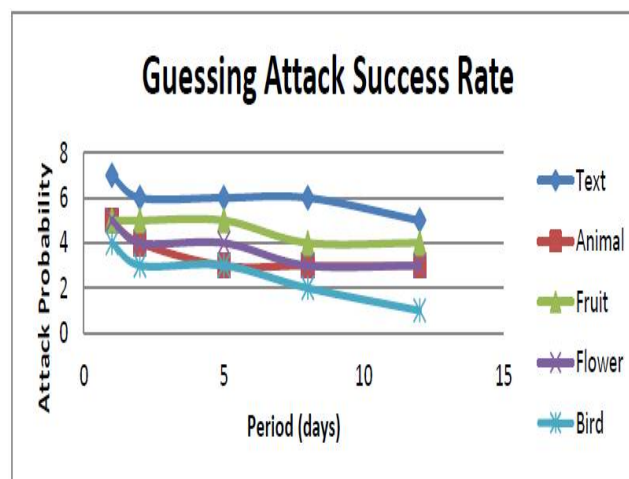


Fig7. Guessing Attack Success Rate

VIII. CONCLUSION

We have proposed CaRP, a new security primitive relying on unsolved hard AI problems. CaRP is both a Captcha and a graphical password scheme. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks: a new CaRP image, which is also a Captcha challenge, is used for every login attempt to make trials of an online guessing attack computationally independent of each other. Overall, our work is one step forward in the paradigm of using hard AI problems for security of reasonable security and usability and practical applications.

REFERENCES

- [1] Bin B. 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 FORENSIS AND SECURITY, VOL.9, NO 6, June 2014.
- [2] Hossein Nejati, Ngai-man Cheung, Ricardo Sosa and Dawn C.I.Koh. DeepCaptcha: An Image CAPTCHA Based on Depth Perception. ACM digital Library, March 2014.
- [3] P.R.Devale Shrikala, M. Deshmukh and Anil B.Pawar. Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme. International Journal of Soft Computing and Engineering, Volume-3, Issue-2 May 2013..
- [4] Iranna A M and Pankaja Patil. Graphical Password Authentication using Persuasive Cued Click Point, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol.2, Issue 7, July 2013.



ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

- [5] Nilesh Kawale and Shubhangi Patil. A Recognition Based Graphical Password System. International Journal of Current Engineering and Technology, Vol.4, No.2, Apr 10, 2014.
- [6] Darryl D'Souza Phani, C.Polina, Roman V and Yampolskiy. Avatar Captcha: Telling Computers and humans apart via face classification. IEEE, 2012.
- [7] Robert Biddle, Sonia Chiasson and P.C.van Oorschot. Graphical Passwords: Learning from the First Twelve Year. School of Computer Science, Carleton University, Jan 4, 2012.
- [8] Mohamed Sylla, Gul Muhammad, Kaleem Habib and Jamaludin Ibrahim. Combinatoric Drag-Pattern Graphical Password. Journal of Emerging Trends in Computing Information Sciences, Vol.4, No.12, Dec 2013.