

HARD AI GRAPHICAL PASSWORD USING CAPTCHA.

Niranjay Gadiwan ,Vikrant Mate.

Under guidance of Prof. Sonali Mastade

Computer Engineering, ZCOER, Narhe, Pune-411041.

Abstract — Many security primitives are based on hard mathematical problems. Use of hard AI problems for security is come into picture with impressive new pattern, but it is not completely explored. There are so many problems which are easy to solve for human brain but it is very difficult to solve for machine. For Example rotate the object by random degrees and with randomly chosen background. This application is mainly used to differentiate between human and machine apart and to solve the “Hard AI Problem”. It also increases the security level and prevents the important data from threats by providing three levels of security. We present a new security originally based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we refer as “Captcha as graphical passwords (CaRP)”. CaRP is both a Captcha and a graphical password scheme.

Keywords- Graphical Password, CaRP, Captcha, Security Primitive, password guessing attack.

I. INTRODUCTION

Completely Automated Public Turing test (CAPTCHA) is use to tell Computers and Humans Apart. Hard AI Problems are problems which easily solve by human intelligence and which are difficult to solve by machine. Using hard AI problems for security is becoming visible as an exciting new paradigm, but this result has been under-explored. This application, presents a new approach which is basically based on hard AI problems, which is a group of graphical password systems put up on top of Captcha technology. This technology we refer as “Captcha as graphical passwords (CaRP)”. CaRP indicates both Captcha and a graphical password scheme. The graphical-password technique is also called as graphical user authentication (GUA). CaRP determine a number of security problems, For Example online guessing attacks, relay attacks.

II. RELATED WORK

In this application the system is providing three levels of security using Captcha as a Graphical Password based on Hard AI Problems.

To provide access to important data to the authenticated user three levels of security are provided.

The levels of security are as follow:

3.1. Level 1:

3.1.1. User Login

AES Algorithm

The advance Encryption Standard Algorithm is used to encrypt the data. In this system AES algorithm is used to store user password in encrypted format.

3.2. Level 2:

3.2.1. First Level Captcha

At this level system will randomly generate one of the following type of captcha.

Grid Structure

Here users have to select the images according to question provided by system from dynamic grid structure of images.



Figure 1. Grid Structure

Rotation Based

Here system will provide a tilt object to user and user have to make it straight by rotating it clockwise or anticlockwise.

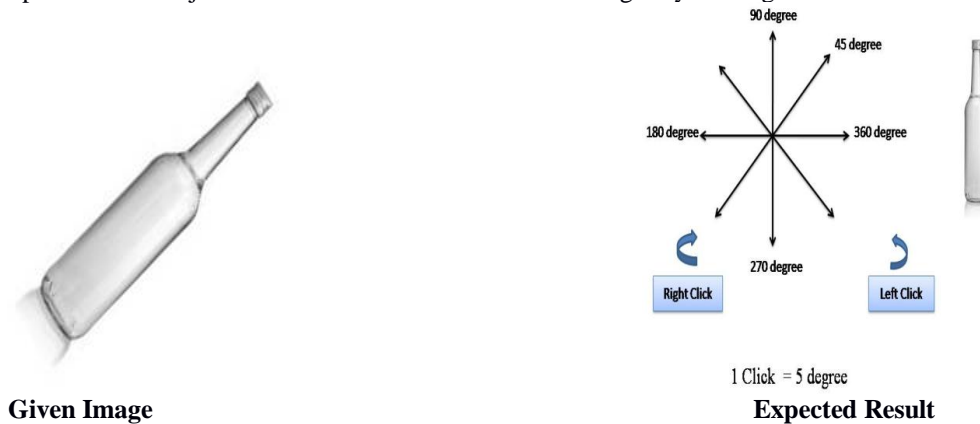


Figure 2. Rotation Structure

3.3. Level 3:

3.3.1. Second Level Captcha

At this level system will randomly generate one of the following captcha.

8-Queens Problem

Here system will provide 8*8 matrix with four answer queens placed and user have to place other queens for solution to the problem.

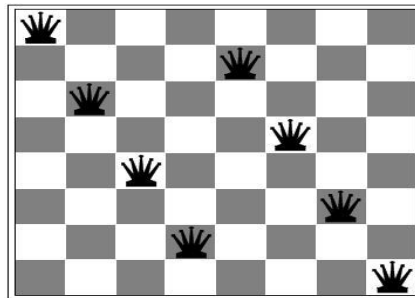


Figure 3. Queens Structure

16-Queens Problem

Here system will provide 16*16 matrix with eight answer queens placed and user have to place other queens for solution to the problem.

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 FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014.
2. Firkhan Ali Bin Hamid Ali Farhana Bt. Karim, "Development of CAPTCHA System Based on Puzzle", IEEE 2014 International Conference on Computer, Communication, and Control Technology (I4CT 2014), September 2 -4, 2014.
3. Chii-Jen Chen You-Wei Wang Wen-Pinn Fang, "A Study on Captcha Recognition", Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing IEEE 2014.
4. Rich Gossweiler Maryam Kamvar Shumeet Baluja, "What's Up CAPTCHA? A CAPTCHA Based on Image Orientation", International World Wide Web Conference Committee (IW3C2) April 20–24, 2009.
5. Colin Hong, Bokil Lopez-Pineda, Karthik Rajendran, Adrià Recasens, "Breaking Microsoft's CAPTCHA", May 2015.