ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

An Efficient Authentication System Using Captcha on Hard AI Problems

Pranita Medankar, Snehal Bane, Mrunalini Girme, Pooja Walke

UG Students, Dept. of Computer Engineering, MES College of Engineering, Pune, India

ABSTRACT: In order to provide best security primitives against bots and online dictionary attacks using hard AI problems for security is emerging as an exciting new approach, but this solution has been under-explored. In this paper, we are presenting a new security primitive based on hard AI problems which is a novel family of graphical password systems built on top of Captcha technology , this technology we called as Captcha as graphical passwords (CaRP). CaRP denotes both Captcha and a graphical password scheme. The graphical-password approach is sometimes called as graphical user authentication (GUA). CaRP species a number of security problems altogether, such as online guessing attacks, relay attacks. If CaRP is combined with dual-view technologies, shoulder-surng attacks are addressed. Especially, the CaRP password even if it is in the search set it can be found only probabilistically by automatic online guessing attacks. CaRP also has many interesting approaches to address the well known image hotspot problem in popular graphical password systems, such as PassPoints, that often leads to password choices that are weak. CaRP is not a modular option, but it offers security and usability and appears to deal with some practical applications for improving online security.

KEYWORDS: Captcha, Graphical password, Password, CaRP, Dictionary attack, Password guessing attack, security primitives, hardAI .

I. INTRODUCTION

While designing a system the important task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. In this paper, we present a new security primitive based on hard AI problems which belongs to the family of graphical password systems built on top of Captcha technology. This technology we call as Captcha as graphical passwords (CaRP). CaRP specifies both Captcha and a graphical password scheme. The main aim is to make the application more secure than the existing application, by using Captcha as a Graphical Password using Hard AI problem. We introduce captcha as an automated test that humans can pass, but current computer programs can’t pass any program that has elevated success over captcha can be used to solve an unsolved Artificial Intelligence (AI) problem. In this paper we provide numerous novel constructions of captcha. The captcha have many applications in practical security. Much like research in cryptography has made a good impact on algorithms for factoring and discrete log, we hope that the use of hard AI problems for security purposes allows us to introduce advance Artificial Intelligence. Two preliminaries of AI problems are introduced. They can be used to construct captcha’s and we show that solutions to such problems can be used for steganographic communication.

II.RELATED WORK

In [3] states about CaRP, a new security primitive depends on unsolved hard AI problems. CaRP is a combination of both Captcha and a graphical password system. The view of CaRP introduces a new idea of graphical passwords, which acquired a new level of approach to defy mainly online guessing attacks a new raise of CaRP image, which is also, seems like a Captcha challenge, it is used for every login challenge to make trials of an online guessing attack computationally autonomous of each other including of brute-force attack too. Although the main argument for graphical passwords is that people are good at remembering graphical passwords than text-based passwords [4].

DOI: 10.15680/IJIRCCE.2017. 0501063

Captcha is used to protect sensitive user inputs on an untrusted client [5]. This techniquesecures the communication Channel between user and Web server from key loggers and spyware, while CaRP is a family of graphical password schemes for user authentication.

III. LITERATURE SURVEY

A CAPTCHA is a program that can generate and tests that most humans can pass, but computer programs cannot pass. Captcha finds the difference between humans and bots in solving the hard AI problems. Such a program can be used to differentiate humans from computers. According to such representation, the text based captcha cannot justify the particular user is human being as it completely determines the captcha pattern which will be in the form of sequence of non-characters. Such type of captcha consists of lack of background noise, distortion of characters or word images and extreme crowding of adjacent character. So for justifying between human being and bots the graphical passwords are considered.

IV. IMPORTANCE OF CAPTCHA

The system which includes captcha as a graphical password is used for authentication of user in order to avoid the login from bots. This will simply specify that the different pattern which can be solved easily by human beings. Such types of problems are quite hard for bots to solve and proceed to the next process. So such types of graphical passwords (like Grid captcha and N Queen's problem) can be used in order to avoid the login from bots or machines. There are two types of CAPTCHA: first is Text Captcha which mainly focuses on recognition of non-character objects and second is Graphical captcha which mainly referred as Image Recognition Captcha (IRC) and it relies on recognition of images.

V. TYPES OF CAPTCHA

1. Text captcha:

This is one of the basic type of captcha which simplify the basic authentication level for recognizing the user. According to this, PayPal and Microsoft Captcha are both composed of background noise and random character strings to avoid automated attacks. The Captchas used by Google, Yahoo all share similar properties: such as a lack of background noise, distortion of characters or word images and extreme crowding of adjacent character. The ability of human to read the random Captcha images is captured by site in the form of pixel, marginal probabilities and site by site covariance. EZ-Gimpy uses word images which employ and determine the character distortion and clutter.

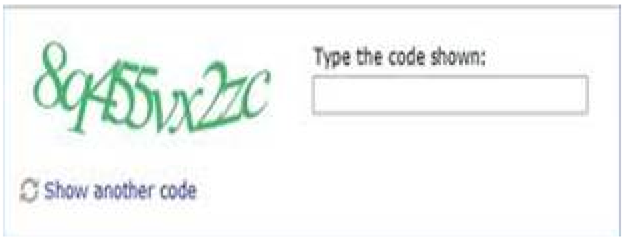
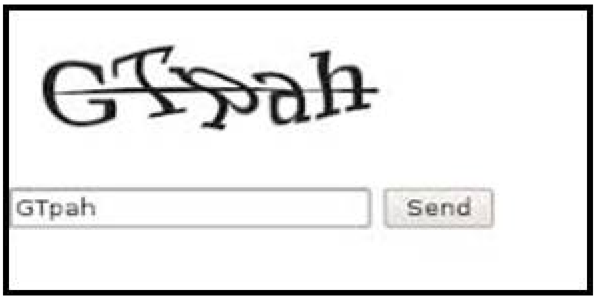


Fig: Basic text based captcha

2. Graphical password:

This type of captcha consists of graphical patterns for recognization. For determining the user the graphical password provide the most simple and impactful password patterns which represents the captcha patterns. Generally Images are more easier and most probably preferred to be remembered than text. In addition, if the number of possible images is enough large, the possible password space which is assembled for graphical password scheme may goes increase as compared to text-based schemes and therefore the system may offer better performance towards dictionary attacks.



GTpah

Fig: Text captcha for recognition of non-character object

3. Grid based Captcha:

These Captcha consist of combination of images which can be represented by using simple grid (having dimentions as n*m). The task of user is to recognize the images given to him to solve the given puzzle. As shown in the below figure, the grid contains 9 images. And the user have to select pictures of a particular object (such as images of beach in the below grid) as a passward characters.

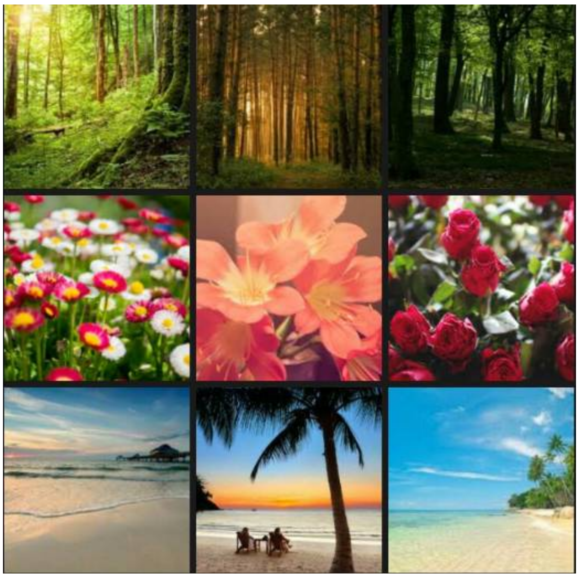


Fig: Grid based Captcha

4. Rotation based Captcha and hardAI problem such as finding solution on N Queen problem:

This type of captcha consists of object rotation which mainly emphasizes on rotation of object in order to get a proper position. As in case of human being, it is easy to recognize the object position by simply determining the actual position after rotation of object. But in case of bots or machine it is quite hard to recognize the proper position of object. So this will easily denies the bots to proceed for the next process.

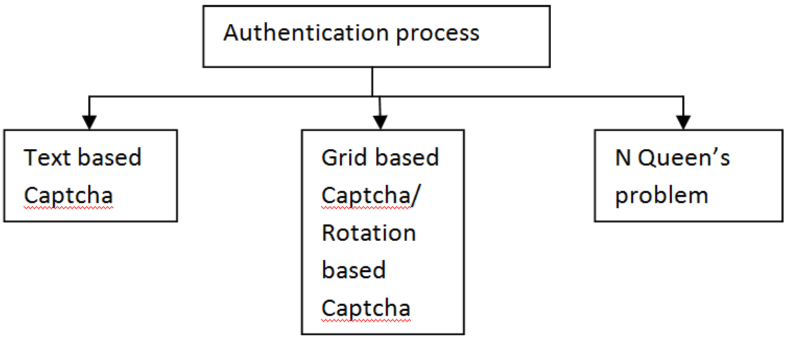


Fig: Block Diagram

VI. PROPOSED SYSTEM

The proposed system consists of graphical password such as, Rotation based captcha and Grid based captcha on second level. So instead of using basic text based captcha this level captcha provide more useful and more realistic way to handle and recognize the user. The solutions on hardAI problems such as N Queen's problem and 8 Queen's problem can be found in order to evaluate the overall procedure of recognizing the user i.e. login from bots or the human being.

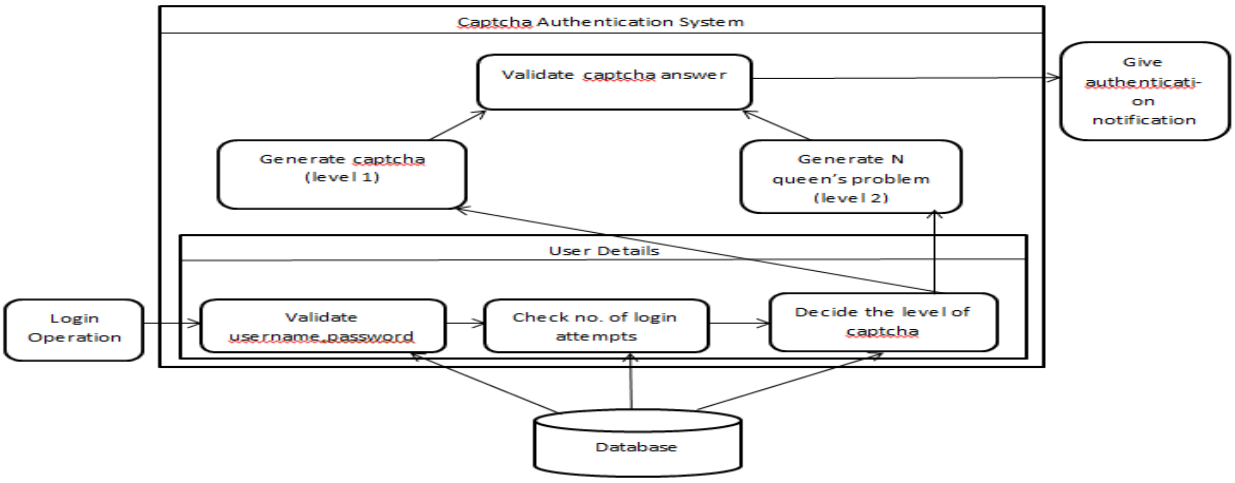

Captcha Authentication System
Validate captcha answer
Give authenticati-on notification
Generate captcha (level 1)
Generate N queen's problem (level 2)
User Details
Login Operation
Validate username,password
Check no. of login attempts
Decide the level of captcha
Database

Fig: Architecture Diagram

VII. METHODOLOGY

We are proposing the system as shown in the figure. There are two levels of captcha and authentication phase as shown in figure.

1. Login authentication:

In login operation, user will enter username and password. Then it will be validated with stored data in database if password and username are valid then user will pass the authentication phase and if password and username are invalid i.e. if parameters are not matched with the parameters which are stored in a database then user's login sattempts will be checked. And if 3 attempts are completed then user will be blocked for that login session. After login user will be at first level of captcha authentication. For such authentication we are using AES algorithm.

A. ADVANCED ENCRYPTION STANDARD(AES)

AES is stands for Advanced Encryption Standard and it is a standard of United States for encryption defined in Federal Information Processing Standard (FIPS) 192. AES is a *symmetric* encryption algorithm processing data in block of 128 bits. AES is symmetric as it use same key for encryption, reverse transformation, and the decryption . The only important task is to keep for security is the key. AES may configured to use different key-lengths, there is a standard that defines 3 lengths. So, the resulting algorithms are named as AES-128, AES-192 and AES-256 respectively. It indicate the length in bits of the key. The older standard is DES (Data Encryption Standard). DES is up to 56bits only. To overcome the disadvantages of DES algorithm, the new standard is AES algorithm is used.

The algorithm starts with an **Add round key** step followed by 9 further rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption. While in both the cases it can be considered with exception that each stage of a round the decryption algorithm is the inverse of it and it is a counterpart in the algorithm. The four stages are :

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

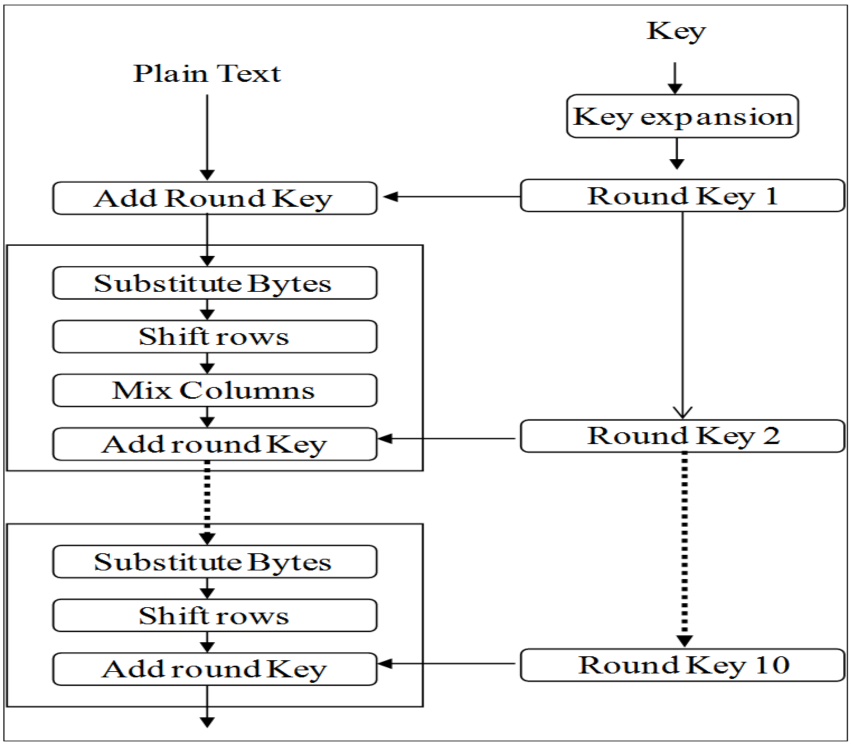


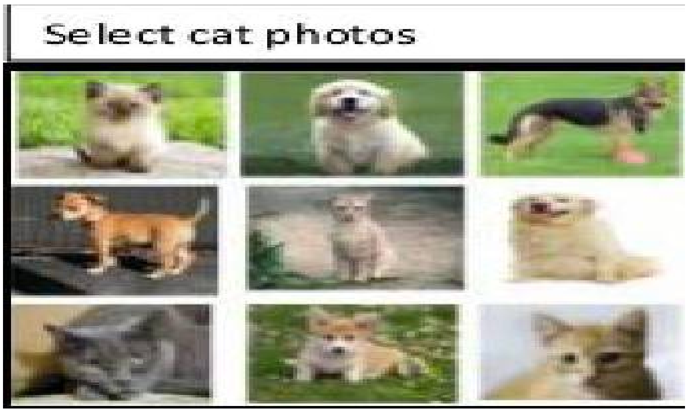
Fig: General structure of AES algorithm

DOI: 10.15680/IJIRCCE.2017. 0501063

The tenth round simply contains the **Mix Columns** stage. The first nine rounds of the decryption algorithm consist of the following 4 stages:
1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns
Again, the tenth round simply contains the **Inverse Mix Columns** stage.

1. First level captcha:
   In first level captcha we are implementing two types of captcha's which are based on hard AI problems. Hard AI problems are those which are easy to solve for human beings but hard for robots machines or bots. As the main motive of captcha is to recognize bots so we are implementing this hardAI problems as captcha thus we can easily differentiate between humans and bots.
   1. ROTATION:
      Rotation of any object can be used as a hard AI problem because guessing whether the object is in straight direction or not is easy for humans but difficult for bots as they didn't know that how objects look in real position. So for solving such problems bots have to know all the attributes of the object. it should have to guess what that object is ,how it looks in its straight position . So storing all such information is complicated for bots.

   2. IMAGE GRID:
      In our project, we are implementing 3*3 matrix image grid captcha. Which contains total 9 images from which user have to guess 3 answer images.



Select cat photos

Fig. 3*3 image grid

Different categories of images will be stored in database as user completes login authentication system will randomly choose any category. Each category will have one question related to that category as shown in above figure, question is to select cat photos. Grid 1,Grid 7 and Grid9 are answer grids thus if user select that grids then only he or she will complete these level.

2. Second level captcha:
   After passing first level of captcha second level of captcha is provided to user. In second level captcha we are implementing N-Queen's problems. N-Queen problem is given to user with some default queens placed. After user solves the problem and submit his answer the answer is verified with answer stored in database. If answer is 'true' then that user is authenticated.

VIII. SYSTEM COMPONENTS

A. HARDWARE COMPONENTS :

Processor	Pentium{|||}
Speed	1.12GHz
RAM	256MB
Hard Disk	20GB
Keyboard	Standard windows keyboard
Mouse	Two or three buttons mouse

B. SOFTWARE COMPONENTS:

Operating System	Windows
Application Server	Tomcat 7
Front End	Java
Scripts	JavaScript
Server side Script	Java Server Pages
Database	MySQL5.0
IDE	Eclipse

IX. CONCLUSION

This paper mainly focuses on solving the Hard AI problem and providing the security to the system. This system provides the security and safety to data. There are so many problem(HARD AI Problem) which are not easily solved by machine at that moment but such a problem can be easily handle by human intelligence. So such a system creates an application which has this feature to handle such a problem. This system gives the authentication to only authorized user. By using Captcha, it will simply differentiate between humans and machines. So these chances of updating or situations of data get hacked by hacker are reduced from system.

REFERENCES

1. Bin B. Zhu, Jeff Yan, GuanboBao, Maowei Yang, and NingXu , “Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems”, IEEE ,Transactions on information forensics and security, vol. 9, no. 6,2014 .
2. Rashmi B J,Prof. B Maheshwarappa, “Improved Security Using Captcha as GraphicalPassword”, IJARCCE Vol. 4, Issue 5, May 2015
3. Ragavendra .A, Jeysree .J, ”Graphical password authentication using CaRP ”,IJARCET, Volume 4 Issue 2, February 2015.
4. Magniya Davis et al, “ Captcha as graphical password”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 148-151.
5. M. Szydlowski, C. Kruegel, and E. Kirda, “Secure input for web applications,” in *Proc. ACSAC*, 2007, pp. 375–384.
6. Firkhan Ali Bin Hamid Ali Farhana Bt. Karim , “Development of CAPTCHA System Based on Puzzle” , IEEE , Communication, and Control Technology (I4CT 2014), September 2 -4, 2014 .
7. Chii-Jen Chen You-Wei Wang Wen-PinnFang , “A Study onCaptcha Recognition”, IEEE , Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2014.
8. Rich Gossweiler Maryam KamvarShumeetBaluja , “What’s Up CAPTCHA? A CAPTCHA Based on Image Orientation” ,IEEE ,MADRID! Track: User Interfaces and Mobile Web /Session: User Interfaces,2009.
9. Colin Hong BokilLopez ,“Breaking Microsoft’s CAPTCHA”, IEEE , Pineda KarthikRajendranAdri‘a Recasens,2015.
10. M. M. VamsiPriya, SushmaNallamalli, D. BhanuPrakash, K. Ramya Sri, “Authentication Using CAPTCHA as Graphical Password”, International Journal of Advanced Research in Computer Science and Software Engineering,2010
11. J. Thorpe and P. C. van Oorschot, “Human-seeded attacks and exploiting hot spots in graphical passwords,” in *Proc. USENIX Security*, 2007, pp. 103–118.
12. P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, “Purely automated attacks on passpoints-style graphical passwords,” *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 393–405, Sep. 2010.