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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

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

Ashwini B. Gade[1], Shubhangi R. Gunjal[2], Megha D. Jadhav[3], Kamal S. Supnar[4], Mohit Dighe[5]

B.E Student, Dept. of Computer Engineering, SCSCOE, Savitribaiphule Pune University, Rahuri Factory, Ahmednagar, Maharashtra, India[1]

B.E Student, Dept. of Computer Engineering, SCSCOE, Savitribaiphule Pune University, Rahuri Factory, Ahmednagar, Maharashtra, India[2]

B.E Student, Dept. of Computer Engineering, SCSCOE, Savitribaiphule Pune University, Rahuri Factory, Ahmednagar, Maharashtra, India[3]

B.E Student, Dept. of Computer Engineering, SCSCOE, Savitribaiphule Pune University, Rahuri Factory, Ahmednagar, Maharashtra, India[4]

Assistant Professor, Dept. of Computer Engineering, SCSCOE, Savitribaiphule Pune University, Rahuri Factory, Ahmednagar, Maharashtra, India[5]

ABSTRACT: Online security is an important issue to tackle. Varioususer authentication methods are used for this purpose. It helps toavoid misuse or illegal use of highly sensitive data. Text andgraphical passwords are mainly used for authentication purpose.But due to various flaws, they are not reliable for data security. Text passwords are insecure for reasons and graphical are moresecured in comparison but are vulnerable to shoulder surfingattacks. Hence by using graphicalpassword system andCAPTCHA technology a new security primitive is proposed. Wecall it asCAPTCHA as gRaphical Password (CaRP). CaRP is acombination of both a CAPTCHA and a graphical passwordscheme. In this paper we conduct a comprehensive survey ofexisting CaRPtechniques namelyClickText, ClickAnimal andAnimalGrid. We discuss the strengths and limitations of eachmethod and point out research direction in this area.[1]

KEYWORDS: Graphical password; CaRP; Captcha.

I. INTRODUCTION

Now a day, vulnerability is a major issue in computer security. Computer and Information security is supported by passwords. The password is used in Authentication process. The traditional authentication method uses text-based password which is also called alphanumeric password, but it has some drawbacks, so graphical password scheme is developed to overcome vulnerabilities of this traditional password scheme[2],[5].

Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. Using a graphical password, users click on images rather than type alphanumeric characters. A key area in security research is authentication, the determination of whether a user should be allowed access to a given system or resource[3],[2]. Traditionally, alphanumeric passwords have been used for authentication, but they are known to have security and usability problems. Today other methods, including graphical passwords, are possible alternatives. This paper reports on research aimed to design a new kind of graphical password system, empirically test its usability, and compare it to alphanumeric passwords. In this concept an image would appear on the screen, and the

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated [3], [4].

The problems of knowledge-based authentication are extremely text-based passwords are well known. Users often needs to create memorable passwords that are easy for attackers to guess, but Strong system-assigned passwords are difficult for users to remember, a graphical password authentication system should encourage users with strong passwords as well as memorable[1].

The main purpose of survey 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[5]. A password of CaRP can be found in a probabilistic way of automatic online guessing attacks. including of brute-force attack too. Hotspots in CaRP images can be no longer be exploited to initiate automatic online guessing attacks, which is an innate weakness in many graphical password systems.

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. HosseinNejati [2] implemented the DeepCAPTCHA: 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 Passfaces. 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 passfaces.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.PankajaPatil [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

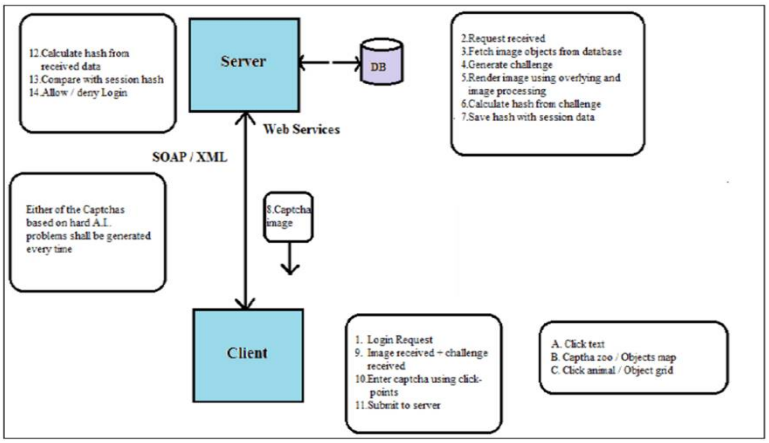

Fig. System Architecture

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

From 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.

IV. PROPOSED ALGORITHM

MD5 Algorithm

Step1 Append padding bits

The input message is "padded" (extended) so that its length (in bits) equals to 448 mod 512. Padding is always performed, even if the length of the message is already 448 mod 512.

Padding is performed as follows: a single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448 mod 512. At least one bit and at most 512 bits are appended.

Step2. Append length

A 64-bit representation of the length of the message is appended to the result of step1. If the length of the message is greater than 2^64, only the low-order 64 bits will be used.

The resulting message (after padding with bits and with b) has a length that is an exact multiple of 512 bits. The input message will have a length that is an exact multiple of 16 (32-bit) words.

Step3. Initialize MD buffer

A four-word buffer (A, B, C, D) is used to compute the message digest. Each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal, low-order bytes first):

word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10

Step4. Process message in 16-word blocks

Four functions will be defined such that each function takes an input of three 32-bit words and produces a 32-bit word output.

F (X, Y, Z) = XY or not (X) Z
G (X, Y, Z) = XZ or Y not (Z)
H (X, Y, Z) = X xor Y xor Z
I (X, Y, Z) = Y xor (X or not (Z))

Step 5. Output

– The message digest produced as output is
A, B, C, D.
– That is, output begins with the low-order byte of A, and end with the high-order byte of D.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

V. EXPECTED RESULTS

In proposed solutionCaRP method based on click points store while the others, to a greater or less extent, made some incorrect submissions. This captcha method gain best human success rate 92%. 75% of test participant say that CARP is easy to use. Or also no complicated operation on password. Or easy to remember than other text or graphical, captcha passwords High Human success rate shows that less chances of requiring multiple attempts of captcha to access account. This comparison shows that proposed CaRP (Captcha as a graphical password) system is user friendly, easy to use, language independent.

VI. CONCLUSION

Alternative to textual password is graphical password. In this paper, a survey over existing graphical password protection techniques and Captcha techniques has been presented. A review over the advantages and limitation of the password protection techniques is also presented. The goal of this research is study the existing graphical password techniques and captcha techniques& develop a new improved graphical password technique combined with a CaRP. CaRP introduces new primitive of graphical password. Also password of system will easy to remember and highly secure. CaRP is built on Captcha technology. which take random images at all time. This survey on existing techniques will help in developing more efficient & secure graphical password based authentication schemes to provide the better security to the user data. The proposed system consists of text password, CaRP authentication scheme and individual graphical password technique. This technique is highly secure. It provides protection from various attacks on the password scheme.

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 FORENSIS AND SECURITY, VOL.9, NO 6, June 2014.

2 HosseinNejati, 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.DevaleShrikala, 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 PankajaPatil. 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.

5 NileshKawale and ShubhangiPatil. A Recognization 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.vanOorschot. Graphical Passwords: Learning from the First Twelve Year. School of Computer Science, Carleton University, Jan 4, 2012.

8 Mohamed Sylla, Gul Muhammad, KaleemHabib and Jamaludinlbrahim.Combinatoric Drag-Pattern Graphical Password. Journal of Emerging Trends in Computing Information Sciences, Vol.4,No.12,Dec 2013.

BIOGRAPHY

Hadyn Ellis. The Science behind Passfaces. www.realuser.com,Feb 2012.