iJRASET
International Journal For Research in
Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 Issue: IV Month of publication: April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4817

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

# Authentication System based on CaRP

Jessica James[1], Sivon Varghese[2], Swati Mupparathy[3], Joylina Almeida[4]
[1, 2, 3]B.E Student, [4]Assistant Professor, Department of Computer Science Engineering, St. John College of Engineering and Management, Mumbai University, India

***Abstract: Security breaching is the main issue faced by the user during authentication. Nowadays online services or Desktop Application come with flaw of security breaching. Old schemes of password consist of some disadvantages like shoulder surfing, hacking of password, password guessing. To overcome the issue of old password schemes, image-based schemes are constructed. Graphical passwords are used to authenticate users in order to avoid security breaching. Human memory is good in visualizing graphical password consists of images and sketches. The key benefits of graphical passwords schemes are improved memorability and to protect against password guessing attack. This paper proposes click based authentication which will protect the system from unauthorised user. In this graphical password and captcha schemes are integrated to form CARP schemes. This improved security mechanism will give user a better security*.**

***Keywords: Graphical Password, Security Primitive, CARP, Recognition Based, Click Based Authentication, Online Password Guessing***

## I. INTRODUCTION

Nowadays, as we can see everything is based on the online systems be it payment, learning, managing the bank accounts, etc. Similarly, our details are more exposed to the outside world. This increases the chance of our personal details getting hacked or misused by attacker. Password cracking is regular practise of hacker's. Password cracking includes practises like shoulder surfing, guessing attacks etc. To overcome such problems raised we use standard internet security to protect users account from being hacked by the hackers and bots. In this paper Graphical password schemes are introduced. Our system is based on click-based captcha as a graphical password which is termed as "CaRP", which reduces chance of human guessing attacks and certain trials if a new click-based image is used for each trial. CaRP is a combination of captcha and graphical password used as entity for secured authentication. Captcha is computably automatic public turing test to tell computer and humans apart. It generates the test which only humans can solve and when captcha is combined with graphical password many more techniques are introduced. In this paper we discuss the strengths and limitations of each graphical password techniques and it also proposes future scope.

## II. IMPLEMENTATION

Authentication schemes are implemented to authenticate user on accessing the website.

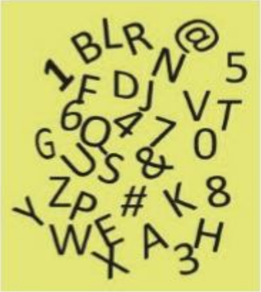
Following are the steps of system flow

*1)* For registration, user must select one of the authentication schemes and then create username and password. Password is created by the user according to their authentication scheme selected at the time of registration.

*2)* For login, user must once again enter his/her username and password based on the selected authentication scheme. click events sequences performed during registration and login process should be matching then only user will be authenticated and get permission to login in to the website.

*3)* User is permitted to the website if and only if he/she is an authenticated user

### *A. Fig of Click text*

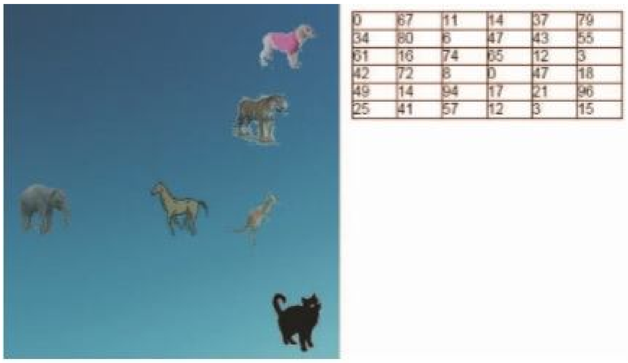


This scheme consists of randomly arranged alphabets in Carp challenge image. This scheme comes under Recognition based scheme.

Steps for click text scheme

1) *Step1:* User registers on system by entering his/her username and password. password will be in random sequence of clicked alphabets. for eg P=”qwertyuiop”
2) *Step2:* To Login in to the system with click text scheme, then user has to provide his/her user name. After that user has to click on the alphabets sequence of the password on the Carp challenged image. Password sequence clicked during registration should be matched with the password sequence clicked during login process.
3) *Step3:* Authenticated user can access the website .

### B. *Fig Animal grid*



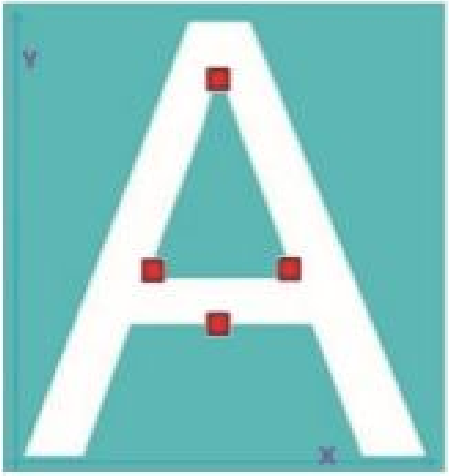
| | | | | | |
|---|---|---|---|---|---|
| 0 | 67 | 11 | 14 | 37 | 79 |
| 34 | 80 | 6 | 47 | 43 | 55 |
| 61 | 16 | 74 | 65 | 12 | 3 |
| 42 | 72 | 8 | 0 | 47 | 18 |
| 49 | 14 | 94 | 17 | 21 | 96 |
| 25 | 41 | 57 | 12 | 3 | 15 |

In this scheme, user provides password which is a sequence of animal names and random number from the table created beside the animal grid. This scheme is combination of click-A-secret and click animal[1].User will get Carp challenged image consisting of 2d animal grid and number grid. Number grid consists of numbers between 1 to 100.In this animal grid scheme ,password is basically click based combination of animal and numbers sequences.

Steps for animal grid scheme

1) User must register in to the system by creating his/her own username and password. password is created by clicking on the grids present in this scheme.
2) User requests for login and then clicks on the password present in the grid. This password is combination of number and animal grid.
3) User gets authenticated if and only if the password clicked during login process is same as the registration process.
4) Authenticated user can access the website.

### C. *Fig. Textpoint 4cr*



In text-point 4cr,Carp challenged image of an alphabet is created and on that click events are performed at any invariant points.

1) *Steps1:* During Registration, User selects the image of an alphabet on which event is performed. User clicks on the invariants points of carp challenged image as his/her password. Authentication server stores the details of the users.
2) *Step2:* During Login, User enters his /her username and password. Password is entered by clicking on the relative positions of the points clicked during registration.
3) *Step3:* Relative position of the points clicked on the carp image during registration process matches with the points clicked during login process than the user is authenticated and can access website.

## III. EXPERIMENTAL ANALYSIS

User plays the key role in graphical password. User should be clever enough while entering the password at the time of login.

### *A. Attack Analysis*

Key logger software attack: In this attack, attacker keeps log of all data entries in key logger software. This type of attack is possible for text-based password. But in our system, we only enter username from keyboard.

### *B. Usability Analysis*

Usability consists of total time required for its execution and ease of schemes for testing our system's performance, we had conducted a survey in which 15- people were requested to use our authentication scheme. We categorize 15- people in different types such as beginners, intermediates and experts according to bell curve theory. By conducting such survey we got to understand the ease of access of these schemes and total time required for execution for each scheme.

### *C. Security analysis on certain attack*

Brute force Attacks: In this type of attack attacker tries many possibilities to crack the password and login in to the system.

1) *For eg:* In textpoint4cr scheme only single alphabet is generated and on that click events are performed. All the click points co-ordinates are different so that attacker fails to login in to the system.
2) *Well studied attack:* Attacker studies about the password schemes and tries many possible combination of different attacks on the system. But, our system consists of password schemes that are multi-factor and randomized. So the attacker fails to study our password scheme.
3) *Shoulder surfing attack:* Attacker uses any digital devices like camera or high resolution video for recording users password. But our system is based on click based carp image so it is difficult to keep track on click events.

## IV. CONCLUSIONS

Graphical password is easy for the people to remember their passwords than text based passwords. We have proposed CARP, CARP is combination of both captcha and graphical password schemes.

CARP includes click text, animal grid techniques and it also include recognition technique like textpoint4cr techniques. It is very difficult for attackers to attack on the system by hacking the CARP-based password because every time new set of images are generated. To increase security images can be produced more at every login attempt. Improvement of CARP techniques can be done by combining two techniques together to produce 3-way Authentication technique for ex: If animal grid and click text are combined together

## V. ACKNOWLEDGEMENT

The heading of the Acknowledgment section and the References section must not be numbered.

Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template.  To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

## REFERENCES

[1] Click and Session Based—Captcha as Graphical Password Authentication Schemes for Smart Phone and Web
Vikas K. Kolekar Assistant Professor, Department of Computer Engineering, Vishwakarma Institute of Information Technology, proc.978-1-4673-7758-4/15/$31.00 ©2015 IEEE.

[2] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in Proc. Eurocrypt, 2003, pp. 294–311.

[3] (2012, Feb.) The Science Behind Passfaces [Online]. Available: http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[4] D. Davis, F. Monrose, and M. K. Reiter, “On user choice in graphical password schemes,” in Proc. 13th USENIX Security Symposium, San Diego, CA, 2004.

[5] R. Dhamija and A. Perrig, “Déjà Vu: A user study using images for authentication,” in Proc. 9th USENIX Security, 2000.

[6] D. Weinshall, “Cognitive authentication schemes safe against spyware,” in Proc. IEEE Symp. Security Privacy, May 2006, pp. 300–306.

[7] P. C. van Oorschot and S. Stubblebine, “On countering online dictionary attacks with login histories and humansinthe- loop,” ACM Trans. Info. System Security, vol. 9, no. 3,2006, pp. 235-258.

[8] J. Elson, J. R. Douceur, J. Howell, and J. Saul, “Asirra: A CAPCTHA that exploits interest-aligned manual image categorization,” in proc. ACM CSS, 2007, pp. 366-374.

[9] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, “The design and analysis of graphical passwords,” in Proc. 8th USENIX Security Symp. ,1999, pp. 1–15.

[10] L.Sobrado and J.C.Birget, “Graphical passwords,” The Rutgers Scholar, An ElectronicBulletin for Undergraduate Research, vol. 4, 2002.

[11] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, “PassPoints: Design and longitudinal evaluation of a graphical password system,” Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.

[12] M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage, “Re: CAPTCHAs—Understanding CAPTCHA-solving Services in an Economic Context,” in Proc. USENIX Security, 2010, pp. 435-452

[13] S. Chiasson, P. C. van Oorschot, and R. Biddle, “Graphical password authentication using cued click points,” in European Symposium on Research in Computer Security (ESORICS), 2007, pp. 359-374.