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 6, June 2016

A New Authentication Security Primitive Using Captcha As Graphical Password

Shende P.S, Prof. Bere S.S.

Student, Department of Information Technology, DGOI, FOE, Daund, Savitribai Phule Pune University, Pune, India

Assistant Professor, Department of Information Technology, DGOI,FOE, Daund, Savitribai Phule Pune University, Pune, India

ABSTRACT: A captcha is used to distinguish the human and computer. Captcha is used for high security reason. But the today many more software can break the captcha. This paper contains the technique called CaRP(Captcha as Graphical Password). This is a combination of captcha and graphical password; it is depend on clicked event of mouse. Carp can avoid the human guessing attacks, online attacks, dictionary attacks, relay attack, shoulder surfing attacks etc. CaRP is depending on artificial intelligence problem. For high performance SHA1 and discretize centralization algorithm is used.

KEYWORDS: Captcha, Carp, Discretized centralization algorithm, Graphical Password, SHA1 algorithm

I. INTRODUCTION

Captcha is used to protect online services from attack. But in today, many more software is available to break the captcha. In this paper carp technique is used for security purpose. CaRP means the combination of captcha and graphical password. This carp technique is based on hard, artificial intelligence problem. Hard artificial intelligence problem means this cannot break by intelligent algorithm

CaRP depends on the event of a mouse, . If we click on the particular image in sequence manner, this is used to generate the graphical password. If we click on the first point in the image, then this co-ordinate point is taken, and then second clicks point will take. For the carp we can select different image for different log in attempt. For every log in, different images are generated for different user this is challenging for carp. Those images are selected by system to log in is not simple image this is a combination of a number of image [1].

Carp is created by combination of image recognition and text captcha [23] [24], In text carp, generated password is sequence of character, but these are not typing the password by keyboard only select the series of character from the whole image by right sequence using click-based method. CaRP method is efficient for online services because this password is not found by any attack But the character password is found easily by online guessing attack. So the carp is a better tool than character password.

II. RELATED WORK

In generally user select the text password, pattern those are easy to remember in mind, but this password are found easily by dictionary attacks. For this reason user select the graphical password but this are also attack by the dictionary attack because user select the password those are easy to remember[6]. This reason we create method and classes in the system this can generate passwords by using the user memory. Those passwords which are created by system is weak, then these are attacked by Dictionary attacks. We use the method of cognitive studies if the user drawn the graphical password. The set of password complexity factor is defined by cognitive studies. For best understand the size of classes and weak password, we use the "Draw-A-Secrete"(DAS) graphical password scheme. We analyze the size of these classes for DAS under convenient parameter choices and show that they can be combined to define apparently popular subspaces that have bit sizes ranging from 31 to 41— A surprisingly small proportion of the full password space (58

DOI: 10.15680/IJIRCCE.2016. 0406365

bits). Our results quantitatively support suggestions that user-drawn graphical password systems employ measures, such as graphical password rules or guidelines and proactive password checking [6]. In another way to develop the graphical password, we use the pass point algorithm. In this method we use the model to identify the similar reason for the user, In the pass point system we can develop the password, this is point choose from the image in the serial manner of the mouse click[8]. This model predicts the likely click points. This enables us to predict the entropy of the click point in the graphical password in the selected image This model we are creating is analyze the selected image is well suited for graphical password or not and this also find out the number of attacks on the selected system. At this stage this selected experiment and the model are small, but the future research on this experiment and model expansion of this is needed [8].

In computer system use password for security is most used. But the weakness in the password this is found easily by dictionary attack. this also found by the automated program running on the system. Mostly in computer system password is used for security purpose, but this is weak security of our system. The user is allowed in the system is the practical problem. But the service provider has the responsibility to solve the problem by using the software as well as hardware. But at the time of problem solving user friendliness is required. this paper suggest a new authentication scheme this is better than conventional authentication scheme [14].
This scheme is better than the traditional authentication scheme. this is easy to Implementation. this scheme also useful for the dictionary attack and the denial of service attack.

In today the increase the use of dictionary attack and the brute force attacks on the remote login services. this type of attack on password is hard to avoid. in the Automated Turing Test (ATTs) is important for identifying the malicious user which are trying to log in different ways [16].

III. IMPLEMENTATION DETAILS

A. **Text password** is the combination of 26 uppercase letters and 26 lowercase letters and 10 special symbol 10 digits (0to9). All this combination of number and the character forming the password of different size. but the maximum limit of password are the 10 character. So the combination of this all number and the character and special symbol password is formed. So this password is easy to attack by the relay attacks, human guessing attacks, online dictionary attacks. This password is easy to remember.

B. **Graphical Password** means the images, these are easy to remember than the character password. Graphical password means different images are used to log in with different user. Character password is hard to remember. Resolution of the graphical password is 10*10 for windows and 600*800 is the normal resolution. So the permutation of graphical password is 480010 this is hard to break.

Fig 1: Graphical Password

A Captcha is programmed this can generate the image. This image is identified by the human easily, but the system does not recognize it. So the Captcha is used for distinguishing the human from the system or bets [6]. this technique will distinguish human users from computer system by facing the challenge. This is used for better security for the internet services

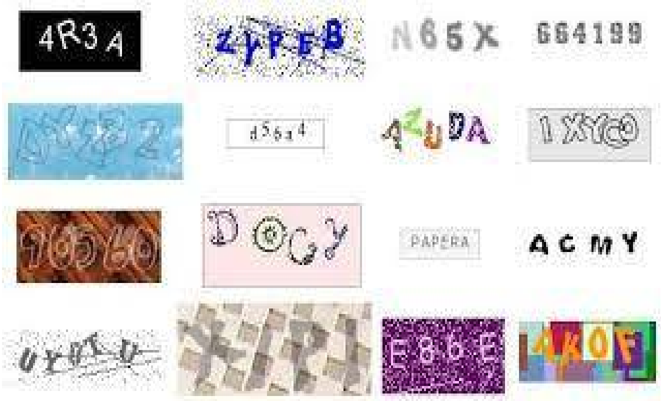
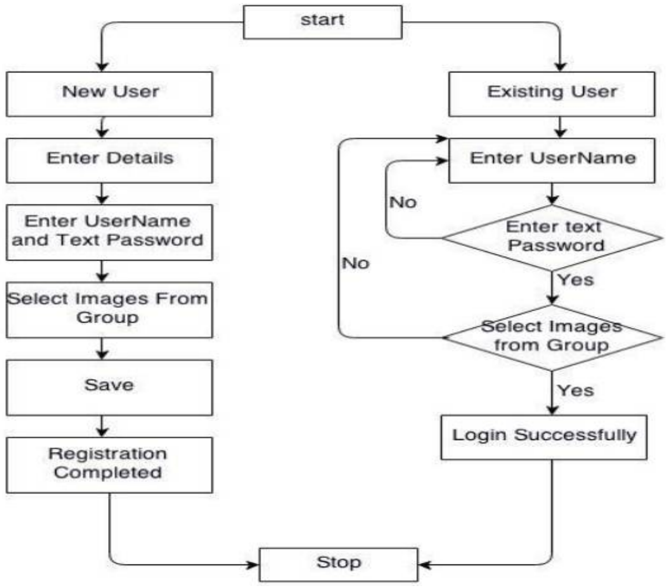


Fig 2: CAPTCHA Password

IV. SYSTEM ARCHITECTURE

In the following architecture there are two possibilities if the user is registered or not. if the user have not registered then first of all user are registered and give the username and password to the user. each user has different password and username. According to this at every log in user will face the captcha challenge by clicking on the correct point on the given image on the particular series user is logged in into the system. The authenticated server receives the password of the particular account and finding out the correctness of this using the SHA-1 algorithm. Authentication is successful if and only if the two hash value is matched.



.

Fig 3: System Architecture

V. MODULE

A. Graphical Password:

In this module, user is giving the authentication image for security purpose to the user. Before the user is accessing the details user have account in that site otherwise those have register first. This also contains the pass point information of the particular image.

B. Captcha in Authentication:

In this model we use the captcha and password for log in into the system. this is called the captcha based password authentication (CbPA)protocol .The CbPA-protocol is use full after the entering the valid pair of password and user ID. CbPA is usefull for the solving the captcha challenge unless the valid browser cookies is received. If the user will enter the user ID and password correct but the they have challenge to solve the captcha.

C. Overcoming Thwart Guessing Attacks:

In the guessing attack, password is guessed by input the password in different manner to the system by using the program those are running on the system automatically. So decrease the counter of password increase the probability of password found. For the avoid this password guessing the new concept is come, this is the graphical password. this password are are hard to guess, This require more trial and error. In this paper we can distinguish the automatic guessing attack and the manually guessing attacks. In Automatic password guessing is based on trial and error basis with respect to program but the manually guessing is based on manually trial and error basis. So the manually password guessing is hard to attack on password.

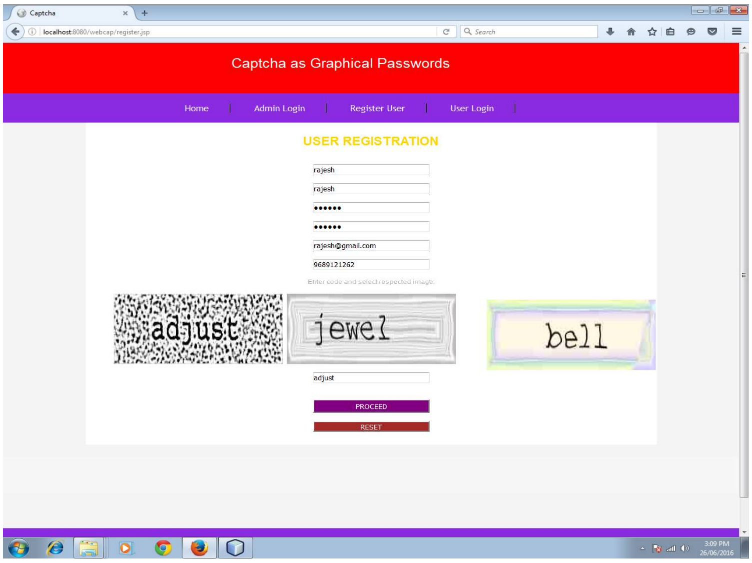
D. Security of Underlying Captcha:

Identifying the object in the CaRP image is the fundamental concept of the CaRP. Captcha process is the approximate process of identifying the object in an image, in this process, not necessary to find out the exact point in the image. object fragmentation of the image is hard, but in the modern text captcha scheme rely on.

Advantage:

- CaRP in important method for security of the password. This protects our password from the online dictionary attack. This is the long term security to our system or online services.
- CaRP also offers protection on shoulder surfing attack, relay attacks, an increasing threat to bypass Captcha protection..

VI. EXPERIMENTAL RESULT



Captcha

localhost:8080/webcap/register.jsp

Captcha as Graphical Passwords

USER REGISTRATION

rajesh

rajesh

••••••

••••••

rajesh@gmail.com

9689121262

Enter code and select respected image:

adjust

Fig 4: User Registration

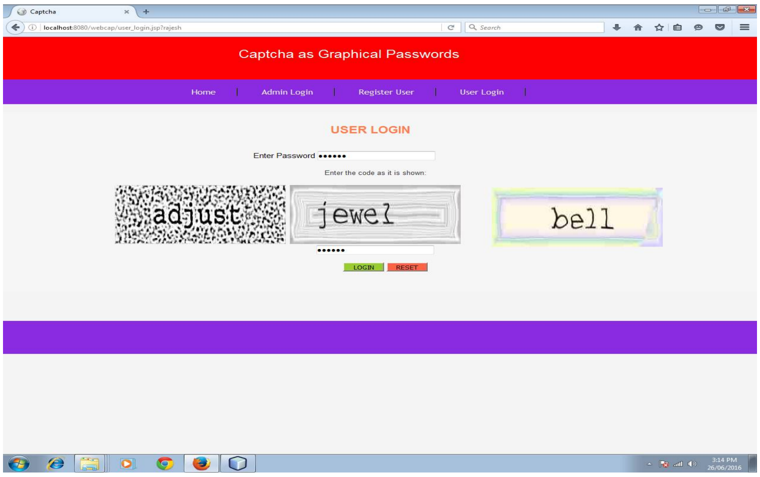
DOI: 10.15680/IJIRCCE.2016. 0406365

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 6, June 2016



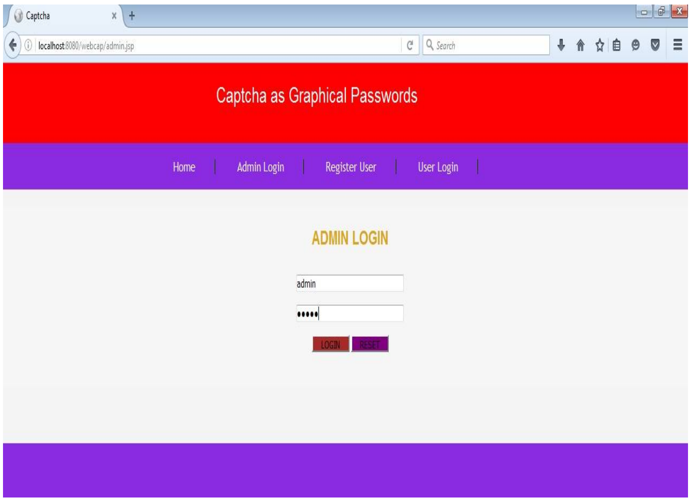
USER LOGIN

Enter Password ••••••

Enter the code as it is shown:

••••••

Fig 5: User Login

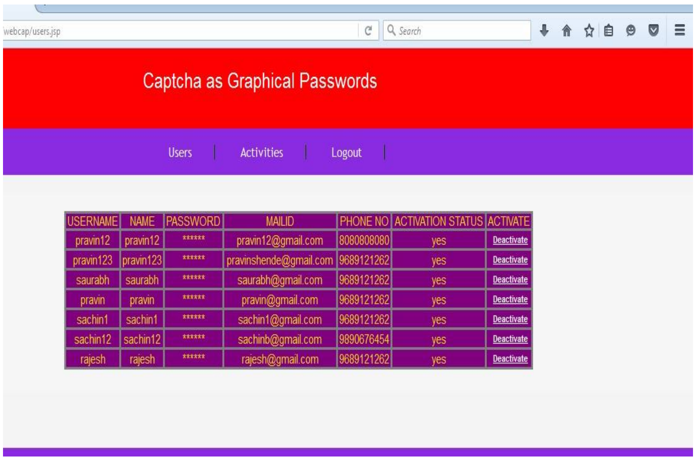

Captcha
localhost:8080/webcap/admin.jsp
Search
Captcha as Graphical Passwords
Home
Admin Login
Register User
User Login
LOGIN
RESET

ADMIN LOGIN

admin

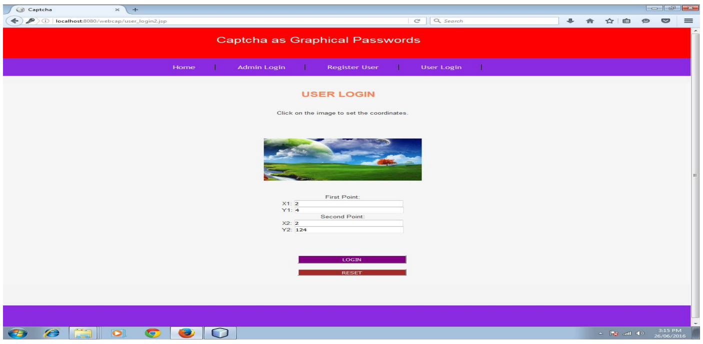
•••••

Fig 6: Admin Login



USERNAME	NAME	PASSWORD	MAILID	PHONE NO	ACTIVATION STATUS	ACTIVATE
pravin12	pravin12	******	pravin12@gmail.com	8080808080	yes	Deactivate
pravin123	pravin123	******	pravinshende@gmail.com	9689121262	yes	Deactivate
saurabh	saurabh	******	saurabh@gmail.com	9689121262	yes	Deactivate
pravin	pravin	******	pravin@gmail.com	9689121262	yes	Deactivate
sachin1	sachin1	******	sachin1@gmail.com	9689121262	yes	Deactivate
sachin12	sachin12	******	sachinb@gmail.com	9890676454	yes	Deactivate
rajesh	rajesh	******	rajesh@gmail.com	9689121262	yes	Deactivate

Fig 7: Admin Activity



Captcha as Graphical Passwords

USER LOGIN

Click on the image to set the coordinates.

First Point:
X1: 2
Y1: 4
Second Point:
X2: 2
Y2: 124

Fig 8: User Login after Activation

VII. CONCLUSION

The goal of the overall project is the security of the system or online services. in this project we use the CaRP image for security purpose. CaRP is the combination of captcha and graphical password. this reason the password does not attack by the any attacker. This password is hard to break, this type password does not found by the computer program or the boots. This system generates the new password at every time, so this is difficult to guess the password.

ACKNOWLEDGMENT

I want to thank all people who help me in different way. Especially I am thankful to my guide “**Prof. Bere S.S.”** for him continuous support and guidance in my work. Also, I would like thank our HOD **“Prof. Bere S. S”**.Lastly, I thank to “**IPGCON-16”** who have given opportunity to present my paper.

REFERENCES

1. M. Alsaleh, M. Mannan, and P. C. van Oorschot, ―Revisiting defenses against large-scale online password guessing attacks,‖ IEEE Trans. Dependable Secure Comput., vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.
2. R. Biddle, S. Chiasson, and P. C. van Oorschot, ―Graphical passwords: Learning from the first twelve years,‖ ACM Comput. Surveys, vol. 44,no. 4, 2012.
3. P. C. van Oorschot and S. Stubblebine, “On countering online dictionary attacks with login histories and humans-in-the-loop,” ACM Trans. Inf. Syst. Security, vol. 9, no. 3, pp. 235–258, 2006.
4. M. Alsaleh, M. Mannan, and P. C. van Oorschot, “Revisiting defenses against large-scale online password guessing attacks,” IEEE Trans. Dependable Secure Comput., vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.
5. 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.
6. S. Chiasson, P. C. van Oorschot, and R. Biddle, “Graphical password authentication using cued click points,” in Proc. ESORICS, 2007, pp. 359–374.
7. S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, “Influencing users towards better passwords: Persuasive cued click-points,” in Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction, vol. 1. 2008, pp. 121–130.
8. D. Davis, F. Monrose, and M. Reiter, “On user choice in graphical password schemes,” in Proc. USENIX Security, 2004, pp. 1–11.
9. Ragavi. V, Dr. G. Geetha , “ CAPTCHA Celebrating its Quattuordecennial – A Complete Reference ” IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 2, November 2011
10. Ved Prakash Singh, Preet Pal “Survey of Different Types of CAPTCHA” Ved Prakash Singh et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2242-2245.
11. T. S. Ravi Kiran, Y. Rama Krishna, “COMBINING CAPTCHA AND GRAPHICAL PASSWORDS FOR USER AUTHENTICATION” IJRIM Volume 2, Issue 4 (April 2012) (ISSN 2231- 4334).
12. 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 891
13. I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, ―The design and analysis of graphical passwords,‖ in Proc. 8th USENIX SecuritySymp., 1999, pp. 1–15.
14. 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.
15. 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.

16. B. Pinkas and T. Sander, “Securing passwords against dictionary attacks,” in Proc. ACM CCS, 2002, pp. 161–170.
17. B. Pinkas and T. Sander, ―Securing passwords against dictionary attacks,‖ in Proc. ACM CCS, 2002, pp. 161–170.
18. P. Dunphy and J. Yan, ―Do background images improve ‗Draw a Secret‘ graphical passwords,‖ in Proc. ACM CCS, 2007, pp. 1–12. [8] A. E. Dirik, N. Memon, and J.-C. Birget, “Modeling user choice in the passpoints graphical password scheme,” in Proc. Symp. Usable Privacy Security, 2007, pp. 20-8
19. 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.
20. 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.
21. P. C. van Oorschot and J. Thorpe, “Exploiting predictability in clickbased graphical passwords,” J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011.
22. T. Wolverton. (2002, Mar. 26). Hackers Attack eBay Accounts [Online]. Available: http://www.zdnet.co.uk/news/networking/2002/03/26/hackers-attack-ebay-accounts-2107350/
23. HP TippingPoint DVLabs, Vienna, Austria. (2010). Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs [Online]. Available: http://dvlabs.tippingpoint.com/toprisks2010