Solving Hard AI Problem using CaRP as Online Network Security

Priyanka Y. Patil
Information Technology
SSBT's COET Bhambhori, Jalgaon
Maharashtra, India
priyankaypatil17@gmail.com

Manju R. Patil
Information Technology
SSBT's COET Bhambhori, Jalgaon
Maharashtra, India
manupatil2793@gmail.com

Nilima R. Barhate
Information Technology
SSBT's COET Bhambhori, Jalgaon
Maharashtra, India
nilima.barhate29@gmail.com

Prashant C. Harne
Information Technology
SSBT's COET Bhambhori,Jalgaon
Maharashtra, India
harneprashant2k7@yahoo.co.in

Ashvini P. Patil
Information Technology
SSBT's COET Bhambhori, Jalgaon
Maharashtra, India
ashvinipatil548@gmail.com

***Abstract*—**Today, there is cut throat competition in Network Security and is major issue in Computer world also several security parameters are based on hard mathematical problems are available to tackle this problem. So many researchers trying to solve this problem from last decades. Using hard AI problems for security is up-and-coming as an exciting new concept so we have to show keen interest in this domain. Hence, in this paper, we are introducing better security parameters based on hard AI problems, explicitly, a novel family of graphical password systems built on top of Captcha technology, which we are proposing Captcha and Graphical Passwords (CaRP). CaRP is both a Captcha and a graphical password system. CaRP sort some security problems, such as online guessing attacks, relay attacks and shoulder-surfing attacks. Especially, a CaRP password can be establish only probabilistically by automatic online guessing attacks even if the password is in the search position. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as PassPoints that often leads to less password choices. CaRP is not a universal solution but it offers reasonable security and usability and it may use few practical applications for getting better online security such as banking, railway reservation etc.

Keywords- *Captcha, CaRP, Graphical password, hard AI problems, hotspot, online guessing attack, passpoint, relay attack.*

*****

I. INTRODUCTION

A new security primitive based on hard AI problems, namely, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password system. CaRP sort some security problems, such as online guessing attacks, relay attacks and shoulder-surfing attacks. Especially, a CaRP password can be establish only probabilistically by automatic online guessing attacks even if the password is in the search position. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as PassPoints that often leads to less password choices. CaRP is not a universal solution but it offers reasonable security and usability and it may use few practical applications for getting better online security such as banking, railway reservation etc.

II. MOTIVATION

Research on the captcha concept is going on from last decades. There are many new concepts related to captcha is coming. In which text-based captcha are more popular. It is a combination of numbers and characters which creates the number of accounts automatically. It shows weak online security. So it is dangerous for online security. So we have to solve this problem, we need to introduce new security system. This problem motivates us to research on strong online security which will better than previous one. This new security system will be based on graphical captcha. It is a combination of captcha and graphical password i.e. CaRP.

III. LITEATUER SURVEY

Bin B. Zhu, et.al.[1] suggested that, some time denial of service attack happen in graphical password scheme that may lock user account so user need expensive head lest cost for account reactivation. It is susceptible to global password attack. The better advantage of this CaRP based security scheme is, it provide protection against online dictionary attack on password, so that it is long time major security intermediation for various online services and it is consider as top cyber security.

Magniya Davis, et.al.[2] proposed survey of the existing graphical password technique and Captcha. The much better advantage of this method is it is difficult to hack. Also Captcha can relies on the gap between human and bots for solving certain hard AI problems. The security of text based Captcha

have been extensively studied and its stated the principle that text Captcha should relay on the difficulty of character segmentation which is computationally exclusive and hard.

P. R. Jayanthi, et.al.[3] proposed if a number of calculations are used to encrypt the password and then this encrypted password can be easily used by the user. This password is nothing but the images so it is easy to remember by the user. A large set of images and a pixel range is provided to each image so the hacker is inefficient to guess the password. A password is much more valuable to hackers than a free email account that Captcha is typically used to protect. Therefore there are more incentive s for attacker to hack CaRP than Captcha.

IV. EXISTING SYSTEM

Captcha is used for online security purpose but now a days the implementation of text based Captcha is very simple. The Captcha is basically used as a computer program or system to distinguish human from machine input during extraction of data from website. It is very useful and requires a large question bank. A primary task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable to identify the correct characters and digits. The text based Captcha is possible to identify the character and digit through Optical character recognition (OCR) technique. Text based Captcha is a combination of characters and numbers that continuously generate the random Captcha by the system but for the human it is somewhat difficult to remember the long string of number and character as a password as compare to the graphical Captcha and also after some day's bots is program which is automatically created the number of accounts of one user which is major problem for security. So here we can say that text based Captcha provides a less security. Hence, there is a need to introduce another strong security scheme which is not easily recognised by the bots.

Fig. 1: Text-based Captcha

Fig. 1 shows a text-based captcha in which captcha is totally based on mathematical problem and it is a combination of numbers and characters.

V. PROPOSED SYSTEM

In this paper, we are proposing a CaRP system which is based on hard AI problem for network security. CaRP provide a better Internet Security Technique to prevent online services such as email and so more from being misuse by bots. In this, we are introducing CaRP which is a combination of both text-based Captcha as well as image-recognition captcha. CaRP is a click based graphical password where the series of clicks on an image is used to gain a password. Nowadays, numbers of graphical password schemes have been proposed and these schemes are classified in three categories based on the task involved in memorizing and entering password such as recognition, recall and cued recall. In recognition based scheme, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he/she selected during the registration stage. In the recall based scheme, a user is asked to reproduce something that he/she created or selected earlier during the registration stage. In cued recall based scheme, the hint is provided for the user to memorize the password and then user can enter the password. Graphics-based Captcha are challenge-tests in which the users have to guess those images that user entered at the time of registration therefore, it is difficult to break this test using pattern recognition technique.

Fig. 2: A ClickAnimal image (left) and 6 × 6 grid (right) determined by red turkey's bounding rectangle.

Fig. 2 shows a ClickAnimal image with an alphabet of 10 animals. Note that different views applied in mapping 3D models to 2D animals, produce many different shapes for the same animal's instantiations in the generated images. Combined with the additional anti-recognition mechanisms applied in the mapping step, these make it hard for computers to recognize animals in the generated image, yet humans can easily identify different instantiations of animals.

CONCLUSION

So from the above survey, we are concluded that today there is cut throat competition in security world. Hence it is harmful to today's technology. So if we develop such type of system then it will provide better results in various applications such as Banking, Online Transaction System, Railway Reservation etc.

REFERENCES

[1] Bin B. Zhu, Jeff Yan, Guanbu 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] Magniya Davis, Divya R, Vince Paul, Sankaranarayanan P N, "CAPCHA as Graphical Password" Magniya Davis et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 148-151.

[3] P. R. Jayanthi, R. Divya, "CAPTCHA AS GRAPHICAL PASSWORD PIXEL BASED PATTERN RECOGNITION SYSTEM" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 11, November 2014.

[4] 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.

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

[6] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008.

[7] 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.

[8] http://www.realuser.com

.