ISSN 2395-1621

The Survey of Graphical Security System by using Captcha

[#1]Hargude Ashwini, [#2]Pacharne Shraddha, [#3]Jagtap Shweta, [#4]Kamble Shivani

[1]ashuhargude12@gmail.com,
[2]pacharneshraddha02@gmail.com.
[3]shwetajagtap13041993@gmail.com,
[4]kambleshivani25@gmail.com

[#1234]Deparment of Computer Engineering
JSPM's, ICOER, Wagholi, Pune.

ABSTRACT

In this paper we propose authentication schemes which consist of graphical password based captchas. It consists of both a captcha and a graphical password schemes. To boost the security aspect to the next level, we contribute some captcha schemes that provide user high security at time of login. Our system provides choice of various authentication schemes to user at time of login. Along with these schemes session based authentication is also provided which will protect system from unauthorized access. We extend the use of captcha as human present recognition as well as graphical password hence it provides all benefits of captcha and make system more powerful from security point of view.

Keywords: Graphical Password, CaRP, CAPTCHA, Authentication, Security

ARTICLE INFO

Article History

Received: 15th November 2016

Received in revised form :

15th November 2016

Accepted: 18th November 2016

Published online :

18th November 2016

I. INTRODUCTION

Nowadays internet acts as an important role. Every person will browse to get their respective necessaries. Internet is useful in many different ways. Everyone desires to browse securely that is they need their personal things to be ensured like passwords or any text file.

As the use of internet develops the hackers are also born, i.e. user's personal documents or passwords are hacked by the third person usually called hackers. As use of internet is important likewise protecting our personals is also an important thing. Here mean to say that there should be an implementation of security for the user's personal documents.

Because of the hackers, every user's personal documents or passwords will be hacked. So then those hackers may use those personals to the bad thing or will share with others for their profit. To overcome these things a strong security should be implemented.

There are different ways for providing security. Here what we introduced is one of the new methods for the security purpose. A new protection primitive is showed based on hard AI troubles, namely, a new family of graphical password schemes built on top of Captcha technology, which is known as Captcha and Graphical Password (CaRP). Here a user while get login to their respective accounts or websites there an image will be generated. The user should click on that image or on any part of that image as a password and that image or clicked particular part will be stored as their graphical password and those images are differently generated for different users.

Considering that generated graphical image as a password along with the user's regular password for further logins. Hence introduce a security for the users so they can browse safely and their personals will be safe.

II. RELATED WORK

User authentication now-a-days is a major problem in authentication system. And for authentication purpose computer security depends on password. There are some important characteristics of password.

1. Password should be changeable.
2. It should quickly and easily executable.
3. It should easy to remember.

Authentication is unavoidable task in security where we use text password as a security technique but text passwords are threaten by many attacks. Such as phishing, brute force attack, dictionary attack etc. among this phishing is a serious threat to text based password. Phishing is an action of getting information such as username, password, contact no. or any other details by masquerading. Another problem with text based password is the difficulty of remembering passwords. To address the problems with traditional username password authentication scheme, an alternative authentication method such as Graphical password is a solution to text based password. Because human ability to recall pictures is more whether they are line drawing object or real object than textual password. In Graphical password user set image instead of text as his password. Because of these above advantages, there is a growing interest in graphical password. In addition to web login application and work-stations, graphical passwords have also been used to ATM machines and mobile devices.

CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is programs that generate tests that are human solvable, but current computer programs do not have the ability to solve them. a captcha is a program that protect sites against bots, resisting automatic adversarial attacks, and it has many applications for practical security, contain online polls, free email services, search engine bots, preventing from dictionary attacks, spam and worms etc.

Problem Statement:
This research aims to study the existing password schemes and to design and develop a new improved graphical password scheme. CaRP is Captcha as a graphical password. With the hybrid use of CAPTCHA and graphical password it can addresses a number of security problems altogether. In information security, user authentication is a major problem in every system. And for authentication purpose every system depends on password whether it is textual password or graphical password. CAPTCHA is a test build by computer programs which human can pass but computer programs cannot pass.

III. LITERATURE SURVEY

[1] L. V. Ahn, M. Blum, Nicholas J. Hopper and J. Langford, CAPTCHA: Using hard AI problems for security, In the Proceedings of Eurocryypt'03, pp.294311,2003, available at: http://www.captcha.net/.
Description: He introduce two families of AI problems that can be used to construct captchas and we show that solutions to such problems can be used for steganographic communication. captchas based on these AI problem families, then, imply a win-win situation: either the problems remain unsolved and there is a way to differentiate humans from computers, or the problems are solved and there is a way to communicate covertly on some channels.

[2] R. Biddle, S. Chiasson, and P. C. Van Oorschot, Graphical passwords: Learning from the first twelve years, ACM Computing Surveys (CSUR), vol. 44, no. 4, p. 19, 2012
Description: He review usability requirements for knowledge-based authentication as they apply to graphical passwords, identify security threats that such systems must address and review known attacks, discuss methodological issues related to empirical evaluation, and identify areas for further research and improved methodology.

[3] D. Davis, F. Monrose, and M. K. Reiter, On User Choice in Graphical Password schemes. In the 13th USENIX security Symposium, 2004.
Description: He show that permitting user selection of passwords in two graphical password schemes, one based directly on an existing commercial product, can yield passwords with entropy far below the theoretical optimum and, in some cases, that are highly correlated with the race or gender of the user. For one scheme, this effect is so dramatic so as to render the scheme insecure. A conclusion of this work is that graphical password schemes of the type we study may generally require a different posture toward password selection than text passwords, where selection by the user remains the norm today.

[4] Dhamija, R., Perrig, A. (2000), Déjà vu: A User Study. Using Images for Authentication, 9th USENIX Security Symposium.
Description: He examine the requirements of a recognition-based authentication system and propose, which authenticates a user through her ability to recognize previously seen images. This is more reliable and easier to use than traditional recall-based schemes, which require the user to precisely recall passwords or PINs. Furthermore, it has the advantage that it prevents users from choosing weak passwords and makes it difficult to write down or share passwords with others.

[5] Partha Pratim Ray, "Ray's Scheme: Graphical Password Based Hybrid Authentication for smart hand held devices,"Journal of Information engineering and Applications, ISSN 2224-5782(print) ISSN 2225-0506(online) vol2, no. 2,2012.
Description: In this paper, he proposed a new hybrid graphical password based system. The system is a combination of recognition and pure recall based techniques and that offers many advantages over the existing systems and may be more convenient for the user. This approach is resistant to shoulder surfing attack and many other attacks

on graphical passwords. This scheme is proposed for smart hand held devices (like smart phones i.e. PDAs, ipod, iphone, etc) which are more handy and convenient to use than traditional desktop computer systems.

IV. SYSTEM FLOW

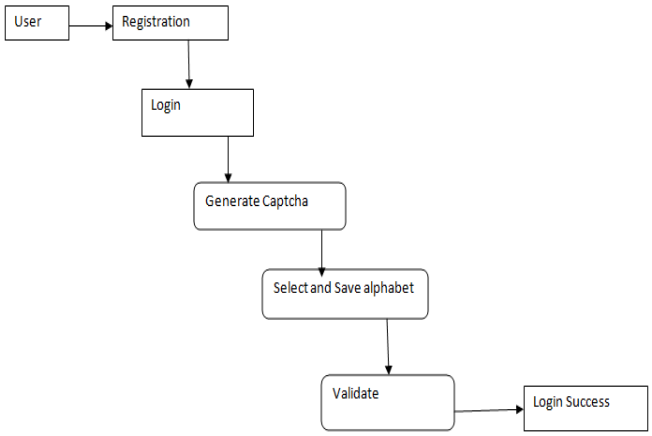

Fig 1. Proposed System flow diagram

The working model of proposed system is shown in figure 1. As the figure says when user requested to register or login to specific pages request is sent to server and server generates the CaRP images. This step consists of converting the Captcha to CaRP and generating graphical images. There are multiple types of images are generated like text images. Generated CaRP images are displayed to user and user clicks on displayed images. Those resulting images are acts as user ID. Server matches the result obtained by the user. If the block matches then user logged in to specified page. Otherwise login or register attempt will failure.

V. CONCLUSION

Here proposed CaRP, a new protection primitive relying on unsolved hard AI problems. The notion of CaRP presents a fresh class of graphical passwords, which adopts a fresh approach to stand online estimating attacks: a new CaRP image, which is too a Captcha task, is used for every login shot to make trials an online estimating attack computationally individual of each other. A password of CaRP can be start only probabilistically by unthinking online guessing attacks counting brute-force attacks, a desired protection property that other graphical password systems lack. In addition to proffering protection from online guessing attacks, CaRP is also immune to Captcha relay attacks, and, if pooled with dual-view technologies.

REFERENCES

[1] L. V. Ahn, M. Blum, Nicholas J. Hopper and J. Langford, CAPTCHA: Using hard AI problems for security, In the Proceedings of Eurocryypt'03, pp.294311,2003.

[2] R. Biddle, S. Chiasson, and P. C. Van Oorschot, Graphical passwords: Learning from the first twelve years, ACM Computing Surveys (CSUR), vol. 44, no. 4, p. 19, 2012.

[3] D. Davis, F. Monrose, and M. K. Reiter, On User Choice in Graphical Password schemes. In the 13th USENIX security Symposium, 2004.

[4] Dhamija, R., Perrig, A. (2000), Déjà vu: A User Study. Using Images for Authentication, 9th USENIX Security Symposium.

[5] Partha Pratim Ray, "Ray's Scheme: Graphical Password Based Hybrid Authentication for smart hand held devices,"Journal of Information engineering and Applications, ISSN 2224-5782(print) ISSN 2225-0506(online) vol2, no. 2,2012.

[6]Shraddha S.Banne, Prof. K.N.Shedge," A Novel Graphical Password Based Authentication Method Using CAPTCHA", International Journal of Informative & Futuristic Research (IJIFR), Volume 2 Issue 11 July 2015

[7] Bin B. Zhu, Je Yan, Guanbo Bao, Maowei Yang, and Ning Xu,``Captcha as a Graphical Passwords A New Security Primitive Based on Hard AI Problems",IEEE Trans, Vol. 9, No. 6, pp 891-904, June 2014.

[8] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, ``Inuencing users towards better passwords: Persuasive cued click -points", in Proc. HCI, British Computer Society, Liverpool, U.K., pp 121-130, 2008.

[9] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen, "Graphical Passwords: A Survey", Department of Computer Science Georgia State University.

[10] A. Dirik, N. Memon, and J.-C. Birget, "Modeling User choice in the Pass-Points graphical password scheme", in 3rd Symp. Usable Privacy and Security(SOUPS), Pittsburgh, PA, pp. 20-28, 2007.

[11] Chippy. T and R. Nagendran, Defences Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points, International Journal of Communications and Engineering, Volume 03 No.3, Issue: 01 March2012 .

