Volume 5, Issue 9, September 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review on Captcha as Graphical Passwords Based on Hard AI Problems

Pooja Pravin Niwalkar*, Prof. N. J. Janwe

Department of Computer Science & Engineering,
Rajiv Gandhi College of Engineering, Research &Technology,
Chandrapur, Maharashtra, India

Abstract*— *Many security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. In this paper, we present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). Consumers tend to choose unforgettable passwords that are easy for aggressors to guess, but strong system allotted passwords are hard for users to recall. Many protection primitives are based on difficult mathematical complications. Utilizing strong AI problems for security is issuing as a stimulating new prototype. A novel protection primitive is introduced based on strong AI problems, namely, a new family of graphical password schemes built up on top of Captcha technology, which is known as Captcha as Graphical Password (CaRP). CaRP deals a number of security troubles altogether, such as online approximating attacks, relay attacks, and, if merged with dual- position technologies, shoulder- browsing attempts. Notably, a CaRP password can be detected alternatively by automatic online estimating attacks still if the password is in the research set. CaRP also offers a new approach to cover the well experienced image hotspot trouble in popular graphical password organizations, such as Pass Points, which often extends to weak password selections. CaRP is not a panacea, but it extends sensible protection and usability and comes out to fit well with some practical lotions for bettering online security.

Keywords*— *Graphical password, hotspots, CaRP, Captcha, dictionary attack, protection primitive.

I. INTRODUCTION

Now a days 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. LITERATURE SURVEY

Robert Biddle, Sonia Chiasson, P.C. van Oorschot have provided a comprehensive overview of published research in the area, covering both usability and security aspects, as well as system evaluation. The paper's catalogues existing approaches, highlighting novel features of selected schemes and identifying key usability or security advantages. We then 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.

Ved Prakash Singh and Preet Pal compared that a captcha may come in various forms like text based or image based CAPTCHA. The Bot operation is similar to reverse "TURING TEST" (given by Alan Turing) where the program acts like judge and the other person acts like user. If the user fails this test then he/she is considered to be a machine otherwise the user is considered to be an authentic user or a human being. There are three basic properties that CAPTCHAs must satisfy .CAPTCHAs should be easy for human user pass ,it should be flexible enough so that a tester machine easily generate and grade it, must be hard enough for a bot to pass.

S.Benson Raj, V.S.Jayanthi have found that Denial of Service is a common threat to network security and is also considered to be an automated network attack. To prevent the system from such kind of attacks the CAPTCHA shield must be implemented in the system to identify the difference between the legitimate user and the fake one. To overcome this problem a new CAPTCHA was introduced called picture based or image based or graphics based CAPTCHA. This CAPTCHA based on images has its own advantages as any malicious program can't perform any type of segmentation through edge detection and thresholding, shape matching and random guessing. In the security analysis process this mechanism has shown better results.

Chen-Chiung Hsieh proposed an innovative image-based CAPTCHA for distinguishing human and computer by embedding versatile characters in the images and in method who they proposed it makes the characters invisible by automated image analysis technologies like scale-invariant feature transform while human can easily distinguish the location of the embedded characters . Their designed mechanism was capable to elude such generous of attacks. For in experiments, 15 users were invited to test the system and the success rate is 86%. If wrong operations like clicking out of text boxes were excluded, the success rate reached 95%. Compare the average logging time with reCAPTCHA and hello CPTCHA, the proposed method is faster than these two methods by 32 seconds and 115 seconds, respectively.

Haichang Gao, Wei Jia, Fei Ye and Licheng Ma have first categorizes existing graphical password schemes into four kinds according to the authentication style and provides a comprehensive introduction and analysis for each scheme, highlighting security aspects. Then they review the known attack methods, categorize them into two kinds, and summarize the security reported in some user studies of those schemes. Finally, some suggestions are given for future research.

Comprehensive Study on Performance Analysis of Various Captcha Systems, author have mentioned a new CAPTCHA which is based on moving object identification and tracking problems. It is referred to biological motion vision model. Based on Edge Mutation an innovative Single-frame Zero-knowledge rule is also put forward to the CAPTCHA generation algorithm. Only after solving the moving object recognition problem successfully an attacker can access the test service system. This kind of animated CAPTCHA is not only able to check the attacks based on static OCR technology but also check the attacks against the moving object detection. Inside the research paper they have mentioned three kinds of programs: the non-visual programs, the visual programs based on OCR problems and visual programs based on non-OCR problems. It most widely used and applied program is based on the visual programs based on the visual programs based on OCR problems with the advantage of implementation and operation. Whenever a user makes a request to the server, the server responds to the user with a picture containing a string of random characters and numbers. The user has to identify the sequence of characters in order to get access to the server resources.

III. PROBLEM FORMULATION

A.The most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge, i.e., a puzzle, beyond the capability of computers but easy for humans. Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots. Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. **A** fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable.

B.This existing paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. Using hard AI (Artificial Intelligence) problems for security, initially proposed in [6], is an exciting new paradigm. Under this paradigm, the most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge.

IV. OBJECTIVE

Following are the objectives to overcome the problem formulation:

A. To offer protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services.
B. To offer protection against relay attacks, an increasing threat to bypass Captcha protection.
C. It offers reasonable security and usability and appears to fit well with some practical applications for improving online security.
D. This threat is widespread and considered as a top cyber security risk. Defence against online dictionary attacks is a more subtle problem than it might appear.

V. PROPOSED METHODOLOGY

The main contributions of this paper are as follows:

A. We present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP).

B. CaRP is both a Captcha and a graphical password scheme. Carp addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Notably, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. 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 weak password choices. CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security**.** We present exemplary CaRPs built on both text Captcha and image-recognition Captcha. One of them is a text CaRP wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaRP images. CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. This threat is widespread and considered as a top cyber security risk. Defence against online dictionary attacks is a more subtle problem than it might appear.

VI. CONCLUSIONS

Thus we have studied various previous types of captcha and have also proposed a new technique using hard AI problems. Therefore our approach combines the advantages of increasing the security and providing authentication along with easy memorable power of password with the help of graphical password.

ACKNOWLEDGMENT

We would like to thank Department of Computer Science & Engineering, RCERT Chandrapur for providing infrastructure and guidance to understand captcha,graphical captcha and its various types.

REFERENCES

[1] 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.

[2] (2012, Feb.). *The Science Behind Passfaces* [Online]. Available:http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[3] 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.

[4] 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.

[5] 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.

[6] 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

[7] D. Florencio and C. Herley. “A large-scale study of WWW password habits”. In 16th ACM International World Wide Web Conference (WWW), May 2007.

[8] H.C. Gao., Z.J. Ren., X.L. Chang., X.Y. Liu., etc., “A New Graphical Password Scheme Resistant to Shoulder-Surfing”, International Conference on Cyberworlds (CW), pp.194-199, December 2010.

[9] J. Thorpe. “On the Predictability and Security of User Choice in Passwords”. PhD thesis, School of Computer Science, Carleton University, January 2008.

[10] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon. “PassPoints: Design and longitudinal evaluation of a graphical password system”. International Journal of Human-Computer Studies, 63 (1-2): 102-127, 2005.

[11] P. C. van Oorschot, A. Salehi-Abari and J. Thorpe. “Purely Automated Attacks on PassPoints-Style Graphical Passwords”. IEEE Transactions on Information Forensics and Security, 5(3): pp.393-405, 2010.

[12] Real User Corporation. *The science behind Passfaces*. White paper, http://www.realuser.com/published/ScienceBehindPassfaces.pdf, accessed Feb. 2012.

[13] Baljit Singh Saini and Anju Bala "A Review of Bot Protection using CAPTCHA for Web Security," IOSR Journal of Computer Engineering, 2013, pp. 36-42, 2013.

[14] Xiao Ling-Zi and ZHANG Yi-Chun "A Case Study of Text-Based CAPTCHA Attacks," in International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover, 2012.

[15] Chen-Chiung Hsieh and Zong-Yu Wu "Anti-SIFT Images Based CAPTCHA Using Versatile," IEEE, 2013.

[16] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, “Against spyware using CAPTCHA in graphical password scheme,” in *Proc. IEE Int. Conf. Adv. Inf. Netw. Appl.*, Jun. 2010, pp. 1–9

[17] J. Bonneau, “The science of guessing: Analyzing an anonymized corpus of 70 million passwords,” in *Proc. IEEE Symp. Security Privacy*, Jun. 2012, pp. 20–25.

[18] J. Elson, J. R. Douceur, J. Howell, and J. Saul, “Asirra: A CAPTCHA that exploits interest-aligned manual image categorization,” in *Proc. ACM CCS*, 2007, pp. 366–374.

[19] R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, “A new CAPTCHA interface design for mobile devices,” in *Proc. 12th Austral. User Inter. Conf.*, 2011, pp. 3–8.

[20] S. Kim, X. Cao, H. Zhang, and D. Tan, “Enabling concurrent dual views on common LCD screens,” in *Proc. ACM Annu. Conf. Human Factors Comput. Syst.*, 2012, pp. 2175–2184.