ISSN: 2321-7782 (Online)
Volume 3, Issue 4, April 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Enhancing the Security Using Captcha as a Graphical Password

Shubhangi G. Hande[1]
Department of Computer Engineering
Prof Ram Meghe College of Engineering and Management
Badnera, Amravati University
India

Dr. M. S. Ali[2]
Prof Ram Meghe College of Engineering and Management
Badnera, Amravati University
India

Abstract: CAPTCHA is now standard security mechanism. CAPTCHA stands for completely automated public Turing test to tell computers and human apart which can differentiate humans from machine. It is used for defending against undesirable bot program. The objective of this paper is to focus on the need of generating new CAPTCHA method by evaluating the limitation of present available CAPTCHA.

Keywords: CAPTCHA, CaGP (CAPTCHA as a Graphical Password), Graphical password, Dictionary attack, security primitive.

I. Introduction

Authentication is heart of secure system. Before involving in online transaction user has to authenticate. If sensitive information is given to wrong identity, the entire security of the system will collapse. The most popular common authentication mechanism is alphanumeric password. It is used for user authentication. Text password is not secure for various reasons. Graphical passwords are more secure and resilient to dictionary attack than text password. CAPTCHA (Completely Automated Public Turing test to tell Computers and Human Apart) is now a standard security mechanism for addressing internet bot program or automated attack and website such as Microsoft, Google and Yahoo have their own CAPTCHA. Many financial Institutions use their own CAPTCHA, to protect their e-banking system from automated attack.

A CAPTCHA is a program that protects websites from bots by generating as well as grading tests that humans can pass that test but current computer programs cannot. Human reads distorted text but computer cannot read distorted text. A good CAPTCHA must be robust as well as human friendly. CaGP (CAPTCHA as a Graphical Password) is a graphical password where a password is derived by using a sequence of clicks on an image. An image which is used in CaGP is CAPTCHA challenge, and for every login attempt a new CaGP image is generated. We present CaGP built on both text CAPTCHA and image-recognition CAPTCHA. Based on this key idea we have proposed the CAPTCHA which will be mirrored and reverse that confuse the cyber criminal. Many e-banking systems have used CAPTCHA for user logins. The operating cost of spammer is increased by CaGP and it help to reduce spam emails. For an email service provider which uses CaGP, a spam bot cannot log into an email account if it doesn't know the password.

II. Problem Defination

We present a new security primitive which is based on hard mathematical problem .CAPTCHA as a graphical password is both CAPTCHA and a graphical password scheme. A number of security problem addresses by CaGP. CAPTCHA are designed to be easy for humans but hard for machines. Most recent research has focused only on making them hard for machines. All the graphical passwords are more secured but some CAPTCHA are break. In this project, we develop the CAPTCHA which will be mirrored and reverse that confuse the cyber criminal. Many financial institutions have used CAPTCHA to protect their services (e.g., e-banking) from automated attacks.

III. Related Work

Since the concept of a CAPTCHA was widely introduced by von Ahn in 2000, hundreds of design variations have appeared. By far, most are text-based. The computer generates a challenge by selecting a sequence of letters and distorting the image. CAPTCHA using texts are popular because they are simple, small, and easy to design and implement.

In [1]Bin B. Zhu, Jeff Yan present a new security primitive based on hard AI problems, namely, a family of graphical password systems built on top of CAPTCHA technology, which called as a CAPTCHA as graphical passwords (CaRP). CaRP is both a CAPTCHA and a graphical password scheme. A number of security problems address using CaRP, such as online guessing attacks as well as relay attacks and if combined with dual-view technologies, shoulder-surfing attacks**.** There are many different ways a user can be authenticated by a system.

In [2] Luis von Ahn, Manuel Blum provides several constructions of CAPTCHA. Since CAPTCHA have many applications in practical security, their approach introduces a new class of hard problems that can be broken for security purposes. Research in cryptography has had an optimistic impact on algorithms for factoring and discrete log, the use of AI problems for security purposes allows field of Artificial Intelligence. The author introduces two families of AI problems that can be used to construct CAPTCHA and they show that solutions to such problems can be used for stenographic communication.

In [3] J. Elson, J. R. Douceur, J. Howell, and J. Saul present Asirra a CAPTCHA that asks user to identify cats out of a set of twelve photographs of both cats and dogs. Asirra is very easy for users. User study shows that it can be solved by humans 99.6% of the time in fewer than 30 seconds. Asirra generates challenges by displaying 12 images from a database of over three million photographs that have been manually classified as cats or dogs. Asirra also has several disadvantages: Most CAPTCHA is implemented as stand-alone program libraries that can be integrated into a web site without introducing external dependencies. In contrast, Asirra, like PIX, is both an algorithm and database there is only one instance of it. Therefore, Asirra must be implemented as centralized web service that is used to generate and verify CAPTCHAs on demand for every site that wishes to use it.

In [4] the concept of graphical password introduced R. Biddle and S. Chiasson Graphical passwords can be largely classified into three categories that are recognition-based graphical password, cued-recall graphical password, and recall-based graphical password. In recall-based graphical password, users are required to recall a password without any cue a graphical password is the use of a picture and several pictures together to authenticate a user. In recognition-based graphical passwords the user required to recognize and then select a set of preselected images from a larger set. In cued-recall based graphical password, example is that to click a set of points on an image.

In [5] H. Tao and C. Adams the author have taken a new grid-based graphical password scheme PassGo, in which to authenticate to system users select meeting points on a grid. Scheme motivated by an old Chinese game Pass Go, which is famous with its variety and simple rules, and more than 100 million people around world have been played. Pass-Go can be considered as an improvement of Draw a secrete (DAS), as it keeps most of the advantages of DAS and achieves stronger security as well as better usability.

In [6] J.Bonneau develops a partial guessing metrics which includes a new alternative of guesswork parameterized by an attackers desired success rate. Their metric is easy to approximate and directly related for security engineering. The author’s first contribution is to formalize advance metrics for evaluating the guessing difficulty of a distribution of secrete such as password. Second is privacy preserving approach to collecting a password distribution for statistical analysis.

In [7] M.Motoyama, K. Levchenko C.Kanich, D. McCoy G. M. Voelker and S. Savage introduced a Reverse Turing test or CAPTCHA, has become a defense used to protect open Web resources from being exploited at scale. CAPTCHAs can increasingly be understood and evaluated in purely economic terms, the market price of a solution being protected. The author observe the market-side of this question in deepness and then analyzing the behavior and dynamics of CAPTCHA-solving service providers, and their price performance, and the fundamental labor markets driving this economy.

In [8] In H. Gao, X. Liu, S.Wang, and R. Dai, in this paper the author use the CAPTCHA as a graphical password scheme to resist spyware attack. Spyware is software that gathers information about a person or organization without their knowledge and that may send such information to another entity without consumer contest. CAPTCHA uses the algorithm which is based on hard artificial intelligence problem and a text based password scheme to resist dictionary attack. In that scheme user select their own graphical password image which authenticated, user only need to distinguish pass image from decoy image and then enter certain part of CAPTCHA string under the pass image

In [9] S.Li, M.A, U.Khan, S.A.Khayam, S.A.H.Shah and R. Schmitz said many financial institutions like e-banking have used CAPTCHAs to protect their services from automated attacks. A new set of image processing and pattern reorganization technique is projected to break all e-banking CAPTCHA schemes that establish over the internet, as well as there are three e-banking CAPTCHA schemes for transaction verification and 41 schemes is used for login. This e-banking CAPTCHA scheme which is broken is used by thousands of financial institutions worldwide, which are helping hundreds of millions of e-banking customers.

In [10] Jeff Yan, Paul Dunphy, Draw a secret (DAS) is a representative graphical password scheme. It was introduced in that paper they investigate the novel idea of introducing background images to the draw a secrete scheme, In that users were initially supposed to draw passwords on a blank canvas overlaid with a grid. Encouraging results from their two user studies had shown that people aided with background images tended to set significantly more complicated passwords than their counterparts using the original scheme. The background images also concentrated other conventional characteristics in DAS passwords such as symmetry and centering within the drawing grid, further improving the strength of the passwords.

In[11] M. Szydlowski, C. Kruegel, and E. Kirda, this paper the author present two novel server side technique that can be used to enable secure user input. The first technique uses conformation coupon that are bound to sensitive data to ensure data integrity conformation token can either be looked up directly in a code book or they need to be calculated using simple algorithm. The second technique expands graphical input with CAPTCHA to protect the confidentiality and interact of user input against automated attack. In this paper author discuss some common aspect of client side attack against web application.

In [12] R. Lin, G. B. Bell, and Y.K. Lee S.Y. Huang discuss and demonstrate the relationship between system security and user interface convenience in CAPTCHA design. a new CAPTCHA approach is introduce which is intended specifically for mobile device the experimental result suggest that this new CAPTCHA design is user friendly as well as secure. This paper projected a new form of image based CAPTCHA interface design well suited for Mobile device .the design utilized the convenience of the touch screen interface of mobile device.

In [13] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe introduced and evaluated various methods for purely automated attack against passpoint style graphical password for generating these attack .author introduced a graph based algorithm to efficiently create dictionary based on famous passpoint password is a sequence of points chosen by a user in an image that is displayed on the screen.

In [14] B. B. Zhu et al, in this paper author introduced image recognition CAPTCHAs (IRCs). Author examines all IRCs schemes known to us and evaluates each scheme against the practical requirements in CAPTCHA application, such as Gmail and Hotmail present a novel attack on a representative scheme.

In [15] S.Chiassion, Oorschot, P.C.Van and R.Biddle have used cued click point graphical password scheme for including security and usability valuation and implementation. For knowledge supported authentication system the important usability goal is to support user in selecting password of higher security.

In [16] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford introduced a new class of hard AI problem that exploited for security purposes, and introduced the concept of cryptographic community and present a novel construction.

In [17] B. Pinkas and T. Sander uses CAPTCHA to prevent dictionary attack in password system to use both CAPTCHA and password in a user authentication protocol, which they called CAPTCHA based Password Authentication (CbPA) protocol, which is used for countering online password guessing attack

In [18] A.E. Dirik, N.Momen and J.C. Birget build up a model to identify the most likely regions for users to click in order to create graphical passwords in the PassPoints system. Hotspots were broken to mount successful guessing attacks on PassPoints.

In [19] Sushama Kulkarni, Dr. H. S. Fadewar introduce a face detection and recognition CAPTCHA to classify the web user as human or bot. Find Face CAPTCHA is a biometric CAPTCHA that displays a CAPTCHA image containing 7 embedded images.

In [20] Moy, N. Jones, C. Harkless, and R. Potter paper describes two distortion estimation techniques for object recognition that solve EZ-Gimpy and Gimpy-r, two of the visual CAPTCHAs. Visual CAPTCHAs are used to prevent spammers from performing automated techniques in acquiring free email accounts from sites such as Yahoo and to stop automated ticket purchases from Ticketmaster.

In [21] J. Yan and A. S. El Ahmad examine the security of a text-based CAPTCHA designed by Microsoft and deployed for years at many of their online services including Hotmail, Windows Live and MSN.Author report the low cost segmentation attack that achieved success rate of above 90%.

In [22] Dilip Kumar Kushwaha and Harleen Kaur, implemented a practical and safe image CAPTCHA from text, it is not only hard to recognize, but also easy to recognize for humans as well. It also makes full use of drawback of computers in recognizing images from a confused background and making it still very difficult for computer programs to break.

In [23] Monica Chew and J. D. Tygar, UC Berkeley propose and implement three CAPTCHAs based on naming images, CAPTCHAs based on distinguishing images, and identifying an abnormal image out of a set. New metric for evaluating CAPTCHAs, implement all three CAPTCHAs, calculate them both theoretically and in user studies, and that anomaly identification appears to be the most promising approach.

In [25] G. Goswami, B. M. Powell, M. Vatsa, R. Singh, and A. Noore proposes a novel image-based CAPTCHA that combines the touch-based input methods favored by mobile devices with genetically optimized face detection tests to provide a solution that is simple for humans to solve, ready for worldwide use, and provides a high level of security by being resilient to automated computer attacks.

In [26] S. Ravi Kiran, Y. Rama Krishna suggests a hybrid user authentication approach combining CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) and graphical passwords to provide increased security.

In [28] propose IMAGINATION (Image generation for internet authentication) is a system for the generation of user-friendly, attack-resistant, image-based CAPTCHAs. In their system, they produce controlled distortions on randomly chosen images and present them to the user for annotation from a given list of words.

In [29] Jayshree Ghorpade, Devika Patil, Dhanashree Poal and Ritesh Prasad conduct a comprehensive survey of existing CaRP techniques specifically ClickText, AnimalGrid and ClickAnimal.they talk about the strengths and limitations of each method and point out research direction in this area.

Table I

Comparison of different types of CAPTCHA

Types of CAPTCHA	Security provided	Easy/Difficult for use
Text based	Good	Average
Image based	Good	Easy
Video based	Good	Difficult
Audio based	Good	Difficult
Puzzle based	Average	Difficult

IV. Proposed System

The proposed system contains four modules that are graphical password, authentication using CAPTCHA, attacks and security of underlying CAPTCHA.In figure 1. There are three modules that are user, server, and database.as explained in fig. 1.for user registration and user login CAPTCHA image is displayed on user interface which will be mirrored as well as reversed then the user identify the image and CAPTCHA, and then enter the CAPTCHA text in a textbox. The application then check the CAPTCHA

If the user entered the invalid CAPTCHA the login failed automatically. If the user entered valid CAPTCHA then login success and automatically display the user page.

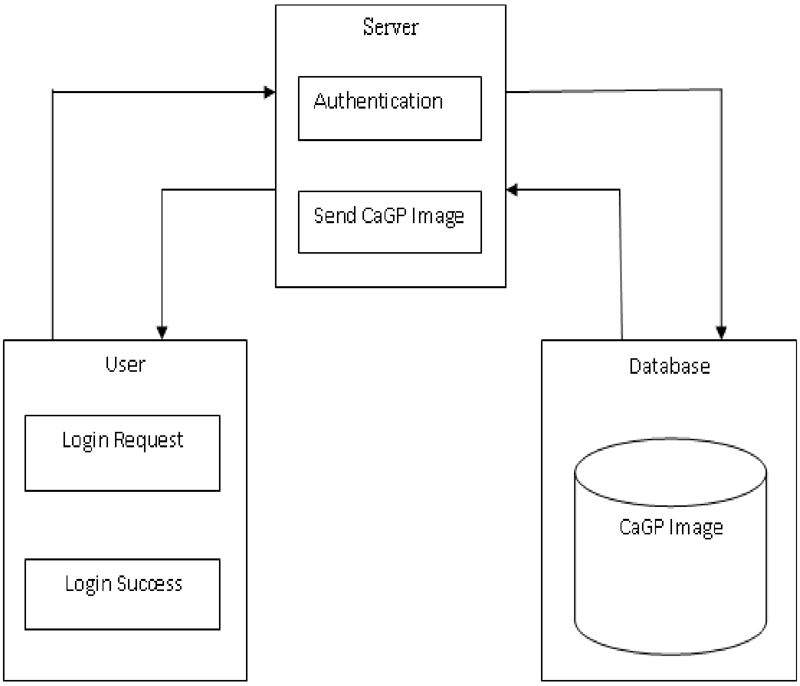

Fig. 1 Proposed System Architecture

V. CONCLUSION

CAPTCHA as a Graphical Password (CaGP) introduces a new family of a graphical password which acts as a firewall for online guessing attack. The proposed work suggests a new technique to display CAPTCHA on the screen which can open new doors to the web security which has become a vital part now days. Also it will give new challenges to the field of Artificial Intelligence.

References

1. 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.
2. Bin B. Zhu and Jeff Yan "Towards New Security Primitives Based on Hard Ai Problems" Microsoft Research Asia, Beijing, China Springer-Verlag Berlin Heidelberg 2013.
3. 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.
4. R. Biddle, S. Chiasson, and P. C. van Oorschot "Graphical passwords: Learning from the first twelve years", ACM Computer. Surveys, vol. 44, no. 4, 2012.
5. H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords", Int. J. Network Security, vol.7, no.2, pp. 273–292, 2008.
6. J. Bonneau, "The science of guessing: Analyzing an anonym zed corpus of 70 million passwords", in Proc. IEEE Symp. Security Privacy, Jun. 2012, pp. 20–25.
7. .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.
8. H. Gao, X. Liu, S.Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA", in Proc. Symp. Usable Privacy Security, 2009, pp. 760-767.
9. S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, "Breaking e-banking CAPTCHAs", in Proc. ACSAC, 2010, pp. 1–10.
10. Jeff Yan, Paul Dunphy, "Do Background Images Improve "Draw a Secret" Graphical Passwords", CCS 07, October 29–November 2, 2007.
11. M. Szydlowski, C. Kruegel, and E. Kirda, "Secure input for web applications", in Proc. ACSAC, 2007, pp. 375-384.
12. 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.
13. 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.
14. B. B. Zhu et al., "Attacks and design of image recognition CAPTCHAs", in Proc. ACM CCS, 2010.
15. S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points" in Proc. ESORICS, 2007.
16. L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in Proc. Eurocrypt, 2003.
17. B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002.
18. A.E. Dirik, N. Memon, and J.C. Birget, "Modeling user choice in the passpoints graphical password scheme" in proc symp, usuable privacy security, 2007, pp 20-28.
19. Sushama Kulkarni, Dr. H. S. Fadewar , "FindFace CAPTCHA: Proposal and Analysis", International Conference on Computer & Communication Technologies 2K14 March 28-29, 2014
20. G. Moy, N. Jones, C. Harkless, and R. Potter, "Distortion estimation techniques in solving visual CAPTCHAs," in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., Jul. 2004, pp. 23-28.
21. J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft CAPTCHA", in Proc. ACM CCS, 2008, pp. 543–554.
22. Dilip Kumar Kushwaha, Harleen Kaur, "Enhancing Web-Security with Stronger Captchas", International Journal of Computer Applications Technology and Research Volume 2, Issue 3, 297-301, 2013
23. Monica Chew and J. D. Tygar, UC Berkeley, "Image Recognition CAPTCHAs", In Proceedings of the 7th International Information Security Conference (ISC 2004), Springer, September 2004, pp. 268-279
24. 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.
25. G. Goswami, B. M. Powell, M. Vatsa, R. Singh, and A. Noore, "FaceDCAPTCHA: Face detection based color image CAPTCHA," Future Generat. Comput. Syst., vol. 31, pp. 5968, Feb. 2014.
26. 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.
27. S. Ravi Kiran, Y. Rama Krishna, "Combining CAPTCHA and graphical passwords for user authentication", International Journal of Research in IT & Management, Volume 2, Issue 4 April 2012.
28. Ritendra Datta, Jia Li, and James Z. Wang, "IMAGINATION: A Robust Image-based CAPTCHA Generation System" November 6–11, ACM 2005.
29. Jayshree Ghorpade, Shamika Mukane, Devika Patil, Dhanashree Poal, Ritesh Prasad, "Novel Method for Graphical Passwords using CAPTCHA", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4 Issue-5, November 2014.

AUTHOR(S) PROFILE

Shubhangi G.Hande received B.E (Computer Science & Engineering) from Sant Gadge Baba Amravati University in 2009 and pursuing M.E. (Computer Engineering) from Sant Gadge Baba Amravati University. Right now working as a lecturer at Prof. Ram Meghe College of Engineering & Management, Badnera–Amravati.

Dr. M. S. Ali completed his B.E (Electronics & Power) from Govt. College of engineering, Amravati, and Nagpur university in 1981 with first division. He completed his M.Tech.in power electronics from IIT Powai, Mumbai in the year 1984.He obtained his PH.D.in electronics engineering from Sant Gadge Baba Amravati University, in the year 2006.His main areas of interest are operating System, Intelligent System and Java technology. He is a recognized Ph.D.guide in Computer Science and Engineering in the faculty of engineering & Technology at SGB Amravati University. He is the founder Principal at Prof Ram Meghe College of Engineering & Management, Badnera-Amravati since 2009.