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. 3, Issue 11, November 2015

A Survey on: Efficient User Authentication using Captcha and Graphical Passwords

Shende Pravin S., Prof.Bere S. S.

P.G. Scholar, Dept. of Information Technology, DGOI, FOE, Bhigwan, Savitribai Phule University of Pune, Pune, India

Professor, Dept. of Computer Engineering, DGOI, FOE, Bhigwan, Savitribai Phule University of Pune, Pune, India

ABSTRACT: The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, user tends to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. In this paper, we conduct a comprehensive survey of the existing graphical password techniques and captcha. 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, graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme .We discuss the strengths and limitations of each method and point out the future research directions in this area. And also major design and implementation issues are clearly explained. The main advantage of this method is it is difficult to hack**.**

KEYWORDS: Graphical password, password, CaRP, Captcha, dictionary attack, password guessing attack, security primitive.

I.INTRODUCTION

The most common computer authentication method is for a user to submit a user name and text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also beeasily guessed or broken. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username password authentication, alternativeauthentication methods, such as biometrics have been used.

CaRP also offers protection against relay attacks, an increasing threat to bypass Captchas protection, wherein Captcha challenges are relayed to humans to solve. Koobface was a relay attack to bypass Facebook’s Captcha in creating new accounts. CaRP is robust to shoulder-surfing attacks if combined with dual-view technologies.CaRP increases spammer’s operating cost and thus helps reduce spam emails. For an email service provider that deploys CaRP, a spam bot cannot log into an email account even if it knows the password. Instead, human involvement is compulsory to access an account. If CaRP is combined with a policy to throttle the number of emails sent to newrecipients per login session, a spam bot can send only a limited number of emails before asking human assistance for login, leading to reduced outbound spam traffic.

II.LITERATURE SURVEY

In commonplace text-based password schemes, users typically choose passwords that are easy to recall, exhibit patterns, and are thus vulnerable to brute-force dictionary attacks. This leads us to ask whether other types of passwords (e.g., graphical) are also vulnerable to dictionary attack because of users tending to choose memorable passwords [6]. We suggest a method to predict and model a number of such classes for systems where passwords are created solely from a user's memory. We hypothesize that these classes define weak password subspaces suitable for an attack dictionary. For user-drawn graphical passwords, we apply this method with cognitive studies on visual recall.

DOI: 10.15680/IJIRCCE.2015. 0311237

These cognitive studies motivate us to define a set of password complexity factors (e.g., reflective symmetry and stroke count), which define a set of classes. To better understand the size of these classes and, thus, how weak the password subspaces they define might be, we use the “Draw-A-Secret” (DAS) graphical password scheme of Jermyn et al. [1999] as an example. 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 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].

We develop a model to identify the most likely regions for users to click in order to create graphical passwords in the Pass Points system. A Pass Points password is a sequence of points, chosen by a user in an image that is displayed on the screen [8]. Our model predicts probabilities of likely click points; this enables us to predict the entropy of a click point in a graphical password for a given image. The model allows us to evaluate automatically whether a given image is well suited for the Pass Points system, and to analyse possible dictionary attacks against the system. We compare the predictions provided by our model to results of experiments involving human users. At this stage, our model and the experiments are small and limited; but they show that user choice can be modeled and that expansions of the model and the experiments are a promising direction of research [8].

The use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by automated programs running dictionary attacks. Passwords remain the most widely used authentication method despite their well-known security weaknesses. User authentication is clearly a practical problem. From the perspective of a service provider this problem needs to be solved within real-world constraints such as the available hardware and software infrastructures. From a user's perspective user-friendliness is a key requirement. In this paper we suggest a novel authentication scheme that preserves the advantages of conventional password authentication, while simultaneously raising the costs of online dictionary attacks by orders of magnitude [14]. The proposed scheme is easy to implement and overcomes some of the difficulties of previously suggested methods of improving the security of user authentication schemes. Our key idea is to efficiently combine traditional password authentication with a challenge that is very easy to answer by human users, but is (almost) infeasible for automated programs attempting to run dictionary attacks. This is done without affecting the usability of the system. The proposed scheme also provides better protection against denial of service attacks against user accounts [14].

Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem. Automated Turing Tests (ATTs) continue to be an effective, easy-to-deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users [16]. In this paper, we discuss the inadequacy of existing and proposed login protocols designed to address large-scale online dictionary attacks (e.g., from a botnet of hundreds of thousands of nodes). We propose a new Password Guessing Resistant Protocol (PGRP), derived upon revisiting prior proposals designed to restrict such attacks. While PGRP limits the total number of login attempts from unknown remote hosts to as low as a single attempt per username, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an ATT. We analyse the performance of PGRP with two real-world data sets and find it more promising than existing proposals [16].

Existing System:

- 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.

Disadvantages of Existing System:

- This existing paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications.

III.PROPOSED ALGORITHM

System Architecture:

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.

The working model of proposed system is shown above figure. As the figure says when user requested to register orlogin 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, 2D and 3D 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.

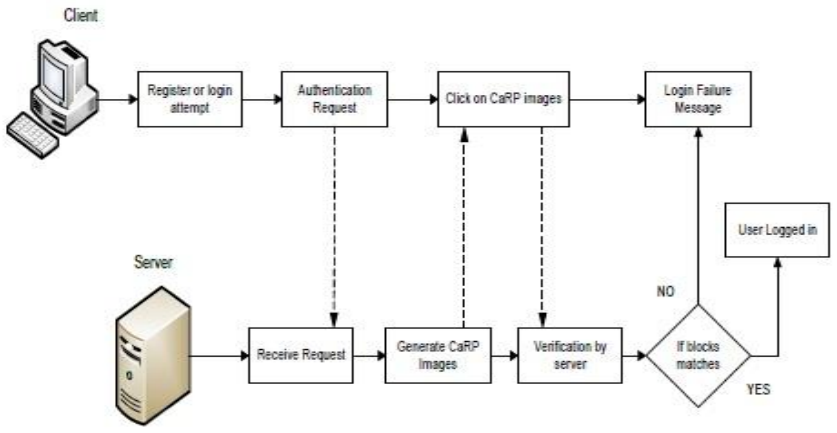

Figure 1: System Architecture of Proposed System

Modules:-

1. **Graphical Password:**
   In this module, Users are having authentication and security to access the detail which is presented in the Image system. Before accessing or searching the details user should have the account in that otherwise they should register first.

2. **Captcha in Authentication:**
   In this module we use both Captcha and password in a user authentication protocol, which we call Captcha-based Password Authentication (CbPA) protocol, to counter online dictionary attacks. The CbPA-protocol in requires solving a Captcha challenge after inputting a valid pair of user ID and password unless a valid browser cookie is received. For an invalid pair of user ID and password, the user has a certain probability to solve a Captcha challenge before being denied access.

3. **Overcoming Thwart Guessing Attacks:**
   In a guessing attack, a password guess tested in an unsuccessful trial is determined wrong and excluded from subsequent trials. The number of undetermined password guesses decreases with more trials, leading to a better chance of finding the password. To counter guessing attacks, traditional approaches in designing graphical passwords aim at increasing the effective password space to make passwords harder to guess and thus require more trials. No matter how secure a graphical password scheme is, the password can always be found by a brute force attack. In this paper, we distinguish two types of guessing attacks: automatic guessing attacks apply an automatic trial and error process but S can be manually constructed whereas human guessing attacks apply a manual trial and error process.

4. **Security of Underlying Captcha:**
   Computational intractability in recognizing objects in CaRP images is fundamental to CaRP. Existing analyses on Captcha security were mostly case by case or used an approximate process. No theoretic security model has been established yet. Object segmentation is considered as a computationally expensive, combinatorially-hard problem, which modern text Captcha schemes rely on.

.

Advantage:

1. CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services.
2. CaRP also offers protection against relay attacks, an increasing threat to bypass Captchas protection.

IV.CONCLUSION AND FUTURE WORK

We have proposed CaRP, a new security primitive relying on unsolved hard AI problems. CaRP is both a Captcha anda graphical password scheme. The notion of CaRPintroducesa new family of graphical passwords, which adopts a new approach to counter online guessing attacks: a new CaRP image, which is also a Captcha challenge, is usedfor every login attempt to make trials of an online guessing attack computationally independent of each other. A password of CaRP can be found only probabilistically byautomatic online guessing attacks including brute-force attacks, a desiredsecurity property that other graphical password schemes lack.

Like Captcha, CaRP utilizes unsolved AI problems. However, a password is much more valuable to attackers thana free email account that Captcha is typically used to protect. Therefore there are more incentives for attackers to hack CaRPthan Captcha. That is, more efforts will be attracted to thefollowing win-win game by CaRP than ordinary Captcha: If attackers succeed, they contribute to improving AI byproviding solutions to open problems such as segmenting2D texts. Otherwise, our system stays secure, contributingto practical security. As a framework, CaRP does not relyon any specific Captcha scheme. When one Captcha schemeis broken, a new and more secure one may appear and be converted to a CaRPscheme.Overall, our work is one step forward in the paradigm of using hard AI problems for security. Of reasonable security and usability and practical applications, CaRP has good potential for refinements, which call for useful future work. More importantly, we expect CaRP to inspire new inventions of such AI based security primitives.

REFERENCES

[1] Bin B. Zhu, Jeff Yan, GuanboBao, 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

[[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] 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.

[4] 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.

[5] 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.

[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] B. Pinkas and T. Sander, ―Securing passwords against dictionary attacks,‖ in Proc. ACM CCS, 2002, pp. 161–170.
[8] 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. 20–28.
[9] 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.
[10] 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.
[11] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in clickbased graphical passwords," J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011.
[12] 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/
[13] HP TippingPointDVLabs, Vienna, Austria. (2010). Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs [Online]. Available: http://dvlabs.tippingpoint.com/toprisks2010
[14] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161–170.
[15] 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.
[16] 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.
[17] 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.
[18] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, 2007, pp. 359–374.
[19] 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.
[20] D. Davis, F. Monrose, and M. Reiter, "On user choice in graphical password schemes," in Proc. USENIX Security, 2004, pp. 1–11.