International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 3 (March'2016)

EFFICIENTLY SECURING SYSTEM USING GRAPHICAL CAPTCHA

K.Gomathi,
Student,
Computer Science and Engineering,
Velammal Institute of Technology,Chennai,India.

K.Mythily,
Student,
Computer science and engineering,
Velammal Institute of Technology,Chennai,India.

S.Poovarasi,
Student,
Computer science and engineering,
Velammal Institute of Technology,Chennai,India.

S.Selvakanmani,
Assistant Professor,
Computer science and engineering,
Velammal Institute of Technology,Chennai,India.

Abstract: This paper proposes a click based Graphical CAPTCHA to overcome the spyware attacks. In case of traditional Text-Based CAPTCHA's user normally enters disorder strings to form a CAPTCHA, the same is stored in the key loggers where spywares can decode it easily. To overcome this, Click-Based Graphical CAPTCHA uses a unique way of verification where user clicks on a sequence of images to form a CAPTCHA, and that sequence is stored in pixels with a random predefined order. Captcha as graphical passwords (CaRP) offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. We are integrating the captcha technology with PCCP (called Persuasive cued click points) or Click based password system for higher security. It offers higher security when compared to the existing Captcha Technology. The password scheme in Graphical Captcha is highly secure and it's better when compared to the existing technology.

Keywords: Graphical password, Relay attack, CaRP, PCCP, dictionary attack, Security Primitive.

I.INTRODUCTION

Security awareness is an important factor in an information security program. While organizations and institutes expand their use of advanced security technology and continuously train their security professionals, fraction of it is used to increase the security awareness among the normal users. As a result, today, organized cyber criminals are trying hard towards research and development of advanced hacking methods that can be used to steal money and secured information from the general public. Password authentication is one of the most common building blocks in implementing access control. Each user has a relatively short sequence of characters commonly referred to as a password. To gain access, providing right password is essential. Common attack for breaking password authenticated systems is dictionary attack [2]. Graphical password is an option for alphanumeric password as text password is slightly hard to remember text password. When any application is provided with user friendly authentication it becomes easy to break and use that application. Cloud security can also be given by alphanumeric password but thing matter is that use of alphanumeric is not that much of secure and easy to remember.

Any individual examining the password can memorize it which may lead to its misuse. Graphical password schemes are more reliable and more resilient to dictionary attacks than textual passwords, but more vulnerable to shoulder surfing attacks [3]. CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is a program that generates and grades tests that are human solvable, but current computer Programs do not have the ability to solve them. The robustness of CAPTCHA is found in its strength in resisting automatic adversarial attacks, and it has many applications for practical security, including free email services, online polls, and search engine bots, preventing dictionary attacks, worms and spam [4]. CaRP is a combination of both a CAPTCHA and a graphical password scheme. CaRP overcome a number of security issues, such as relay attacks, online guessing attacks, and, if combined with CAPTCHA and graphical password, shoulder-surfing attacks. CaRP is click-based graphical passwords, where order of clicks on an image is used to get a new password.

Unlike other click-based graphical passwords, images used in CaRP are used to generate CAPTCHA challenges, and for every login attempt a new CaRP image is generated whether the existing user tries authenticating or a new user. In this paper we conduct a comprehensive survey of existing CaRP techniques namely Click Text, Click Animal and Animal Grid. We point out research direction in this area. We also try to answer our CaRP as secured as graphical passwords and text based passwords. Survey will be useful for information security researchers and practitioners who are interested in finding an alternative to graphical authentication methods.

II.LITERATURE SURVEY

1. Graphical passwords:learning from the first twelve years," *cm comput. surveys*, vol. 44,no. 4, authors name: r. biddle, s. chiasson, and p. c. van oorschot year:2012

Starting around 1999, a great many graphical password schemes have been proposed as alternatives to text-based password authentication. We provide a comprehensive overview of published research in the area, covering both usability and security aspects, as well as system evaluation.

IJCRCST © 2016 | All Rights Reserved

The paper first catalogues existing approaches, highlighting novel features of selected schemes and identifying key usability or security advantages. We then review usability requirementsfor 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.

2. Revisiting defenses against large-scale online password guessing attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 128–141 Authors Name: M. Alsaleh, M. Mannan, and P. C. van Oorschot Year: Jan./Feb. 2012

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. 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 analyze the performance of PGRP with two real-world data sets and find it more promising than existing proposals.

3. A new CAPTCHA interface design for mobile devices," in *Proc. 12th Austral. User Inter.Conf.*, Authors Name: R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee Year: 2011
This paper discusses and demonstrates the interplay between system security and user interface convenience in CAPTCHA design, and in particular, mobile device CAPTCHA design. A CAPTCHA is a computer-based security test used to distinguish human users from artificial users, preventing automated abuse of networked resources. As mobile network services improve, we can anticipate that future mobile network services will come under attack from automated programs. Importantly, while CAPTCHA techniques have existed for Internet services for some time, only limited work has been carried out to establish CAPTCHAs suitable for mobile device interfaces. The Drawing CAPTCHA (2006) is one of the most well known systems of this type. Unfortunately, though it is straightforward, it is not secure. To demonstrate this, an image-processing technique is newly proposed that breaks the Drawing CAPTCHA. A new CAPTCHA approach is then introduced here which is intended speci_cally for mobile devices. Ex-perimental results suggest that this new CAPTCHA design is user-friendly as well as secure.

4.Exploiting predictability in clickbased graphical passwords," *J. Comput. Security*, vol. 19, no. 4,pp. 669–702 Author Name: P. C. van Oorschot and J. Thorpe Year:2011 We provide an in-depth study of the security of click-based graphical password schemes like PassPoints (Weidenbeck et al., 2005), by exploring popular points (hot-spots), and examining strategies to predict and exploit them in guessing attacks. We report on both short- and long-term user studies: one labcontrolled, involving 43 users and 17 diverse images, the other a field test of 223 user accounts. We provide empirical evidence that hot-spots do exist for many images, some more so than others. We explore the use of "human-computation" (in this context, harvesting click-points from a small set of users) to predict these hot-spots. We generate two "human-seeded" attacks based on this method: one based on a first-order Markov model, another based on an independent probability model.

III.EXISITING SYSTEM

This paper proposes a click based Graphical CAPTCHA to overcome the spyware attacks. In case of traditional Text-Based CAPTCHA's user normally enters disorder strings to form a CAPTCHA, the same is stored in the key loggers where Spywares can decode it easily. To overcome this, Click-Based Graphical CAPTCHA uses a unique way of Verification where user clicks on a sequence of images to form a CAPTCHA, and that sequence is stored in pixels with a random predefined order. We are integrating the Captcha technology with PCCP (called Persuasive cued click points) or Click based password system for higher security. It offers higher security when compared to the existing Captcha Technology. The password scheme in Graphical Captcha is highly secure and it's better when compared to the existing technology.

IV.PROPOSED SYSTEM

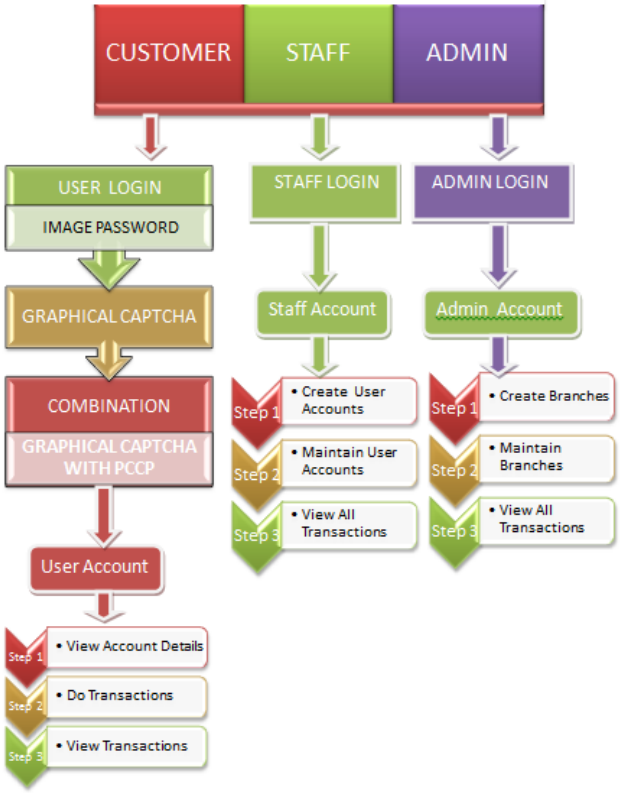
In this paper, we introduce a new security primitive based on hard AI problems, namely, a novel family of graphical password systems integrating Captcha technology, which we call *CaRP (Captcha as gRaphical Passwords)*. CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password.Initially the user derives the sets of password from the uploaded image through click-based-image Password-system,then the User undergoes Graphical image based Captcha challenge where he has to pass the test by clicking appropriate captch images.Since CaRP is combined with secure Click-Based-Graphical-Password-System it enhances the security level to the greater extent.Proposed Technique: *CaRP (Captcha as gRaphical Passwords)* .

ADVANTAGES:

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.
3.CaRP is Highly secure and easy to adopt.

V.ARCHITECTURE DIAGRAM

There were three modules admin login,staff login,user login where in each login we can view all the transactions and In user login we are combining the graphical captcha with the pccp in order to derive the password



VI.REQUIREMENTS

Software Requirements: Operating system - Windows7,Front End-ASP.NET,Coding Language- C# ,Backend-SQL Server 2008
Hardware requirements: ProcessorPentiumDualCore2.00GHZ,
Hard disk - 40 GB RAM -2GB(minimum),

VII.MODULES DESCRIPTION

The project contains Four modules,

- Administrator module.
- Staff module.
- Customer module.
- Graphical Captcha Module

ADMIN MODULE:

This is the first module where the admin can log in to the account by entering the admin name and password

Figure 1 :administrator login

STAFF MODULE:

The staff can login by entering the given username and password. Then, they may create accounts and view all accounts details.

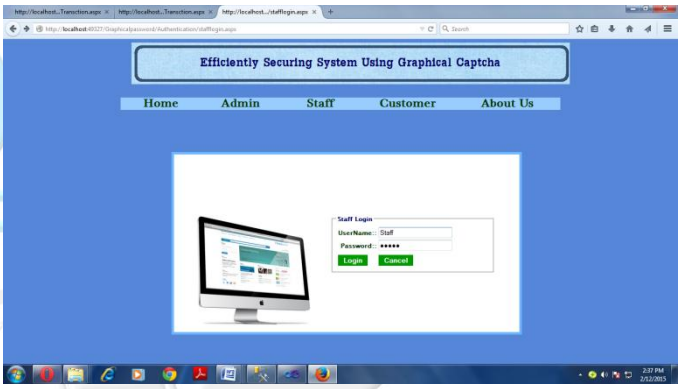


Figure 2: Staff login

CUSTOMER:

Figure 3: customer module

Figure 4: Click Text image

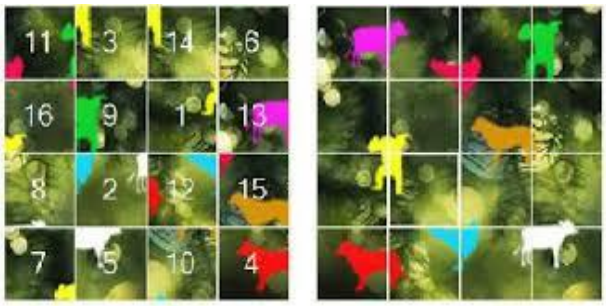


Figure 5: Click Animal images

Figure 6: demonstrates of Click Animal

VIII. CONCLUSION

Our graphical password system provides more security to data and protection against different attack. Our graphical password system is based on picture password and graphical password. For successful login user has to select correct image which is chosen by user during a registration and this system provide picture password which provide more security to data. Future work is based on Pattern.We believe that the fields of cryptography and artificial intelligence have much to contribute to one another. captchas represent a small example of this possible symbiosis. Reductions, as they are used in cryptography, can be extremely useful for the progress of algorithmic development. We encourage security researchers to create captchas based on different AI problems.

IX. REFERENCE

[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 ofgraphical 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] P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawn graphical passwords," *ACM Trans. Inf. Syst. Security*, vol. 10, no. 4, pp. 1–33, 2008.

[7] K. Golofit, "Click passwords under investigation," in *Proc. ESORICS*, 2007, pp. 343–358.

[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.