International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-3
International Conference on Research and Recent Trends in Engineering and Technology. (ICRRTET)
Held on 27th January 2016 organized by **Sai Polytechnic College,** Kinhi Jawade, Yavatmal, Maharastra, India.

Captcha as Graphical Password Security

Sonam.R.Upadhyay; Apurva.S.Narnawre & Prof.Rahul Shahane
Computer Science & Engineering, R.T.M.N.U. Nagpur
Sonamupadhyay757@gmail.com; narnawreapurva01@gmail.com

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 under-explored. In this , 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). 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.

Introduction

The security and usability problems inherent in text-based password scheme have resulted in the development of graphical password schemes as possible alternative. However, most of the current graphical password scheme are vulnerable of spyware which is a program that gathers information about the computers use and relays attacks that information back to the third party. There have been some schemes which have made contributions to the development of graphical password in term of spyware resistance. Using challenge response protocol, they have an advantage in that they are resistant to relay attacks ,even the third party who observes a successful login session cannot perform a relay attack. Though they have a positive effect on protecting user password , they are not yet sufficient to stop attackers from harvesting passwords.

CAPTCHA is used in graphical password scheme to resist spyware. CAPTCHA Completely Automated Public Turing Test To Tell Computers And Human's Apart)is a program that generates and grades test that are human solvable but are beyond the capabilities of current computer programs. CAPTCHA use open algorithms based on hard AI problems and has been discuss in text based password schemes to resist dictionary attack ,we explore captcha in the context of graphical passwords to provide better protection against spyware . As long as the underlying

open AI problems are not solved, captcha is a promising way to resist spyware attacks in graphical password scheme.

Based on this key idea we have proposed a new graphical password scheme using captcha design to be strongly resistant to spyware attack either by purely automated software or via human participation. A preliminary user study indicates that our scheme needs to improve in terms of login time and memorability.

Background and Related Work

1. Graphical Password:

A large number of Graphical Password Schemes have been Proposed.They can be classified into 3 categories according to the task involved in memorizing and entering Passwords: recognition,Recall and crued recall.Each type will be briefly described here.More can be found in a recent review of Graphical Passwords.

Recognition based scheme

A recognition based scheme requires identifying among decoys the visual objects belonging to a password portfolio. A typical scheme is PassFaces where in a user selects a portfolio of faces from a database in creating a password. During authentication, a panel of candidate faces is presented for the user to select the face belonging to her portfolio. This process is repeated several rounds, each round with a different panel. A successful login requires correct selection in each round.The set of images in a panel remains the same between logins, but their locations are permuted.

Recall based scheme

A recall based scheme requires a user to regenerate the same interaction result without cueing. Draw-a-secret(DAS) was the first recall-based scheme proposed.A user draws her password on a 2D grid.The system encodes the sequence of grid cells along the drawing path as a user-drawn password.

Cued-recall scheme

In a *cued-recall* scheme, an external cue is provided to help memorize and enter a password. PassPoints is a widely studied click-based cued-recall scheme wherein a user click a sequence of points anywhere on an image in creating a password, and re-clicks the same sequence during authentication.

2.Captcha

Captcha relies on the gap of capabilities between humans and bots in solving certain hard AI problems. There are two types of visual Captcha: text Captcha and Image-Recognition Captcha (IRC). The former relies on character recognition while the latter relies on recognition of non-character objects. Security of text Captch as has been extensively studied.The following principle has been established: text Captcha should rely on the difficulty of character segmentation, which is computationally expensive and combinatorially hard .Machine recognition of non-character objects is far less capable than character recognition.

International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-3
International Conference on Research and Recent Trends in Engineering and Technology. (ICRRTET)
Held on 27th January 2016 organized by **Sai Polytechnic College,** Kinhi Jawade, Yavatmal, Maharastra, India.

3.Captcha in authentication:

It was introduced in [14] to 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 it 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.Captcha was also used with recognition-based graphical passwords to address spyware [40], [41], wherein a textCaptcha is displayed below each image; a user locates her owpass-images from decoy images, and enters the characters at specific locations of the Captcha below each pass-image asher password during authentication. These specific locations were selected for each pass-image during password creation as a part of the password.

Proposed System

- In this project, 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).
- 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.

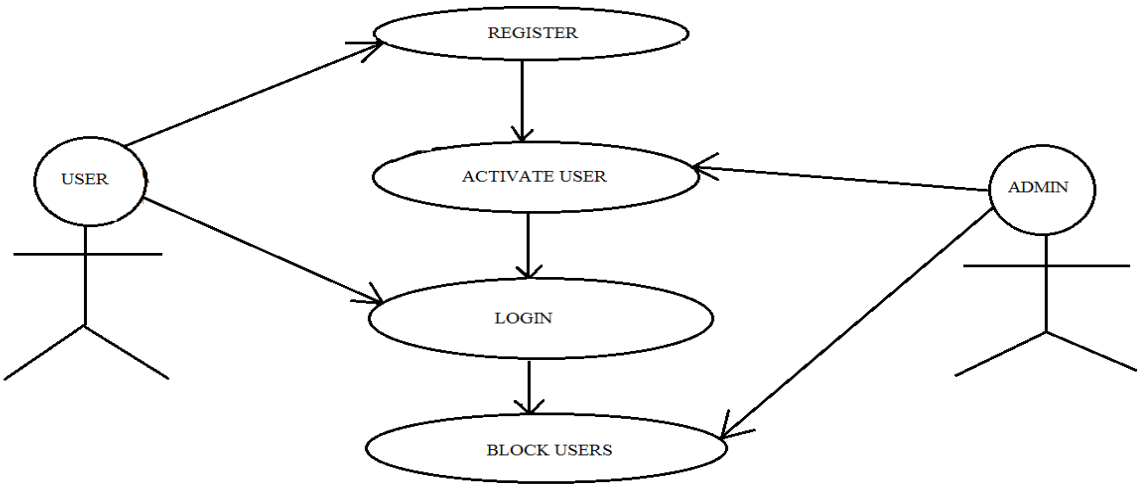

Fig2: Flow diagram

Modules

1.Graphical Password Generation:

In these module,users are having authentication and security to access the detail which is presented in the image system.Before accesing or searching the details the user should have th account in that otherwise they should register first.

2.Captcha in authentication:

It was introduced in [14] to 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 it 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.Thwart Guessing Attack:

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 password.

In this project,we distinguish two types of guessing attacks; automatic guessing attacks apply an automatic trial and error process and error process.

4. Security of underlying Captcha:

Existing analysis on Captcha security were mostly care by care or used an approximate process.No theoretic security model has been established yet.

System Architecture:

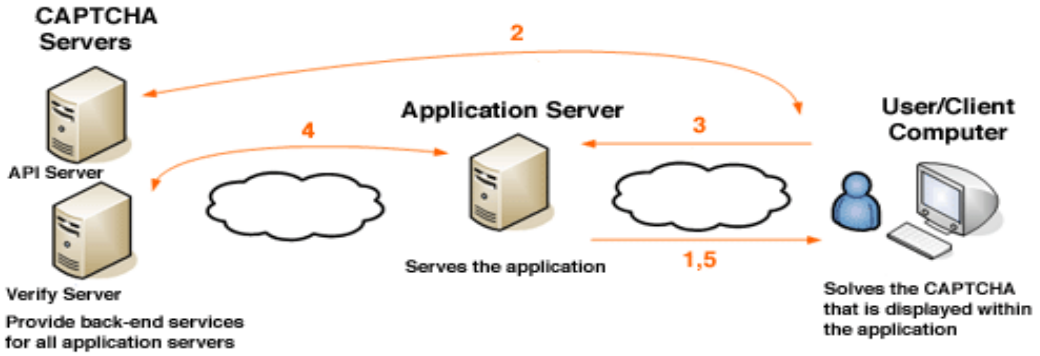

Fig:System Architecture

Advantages of Proposed System

- CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services.
- CaRP also offers protection against relay attacks, an increasing threat to by pass Captcha's protection.

Applications:

- It can be applied on touch screen devices.
- Many e-banking systems uses Captcha in user logins that requires solving a Captcha challenge for every online login attempt.
- CaRP increases spammer's operating cost and thus helps to reduce spam emails.

Future scope:

- In the proposed work a password authentication schemes using associating memories based on normalized combine text and graphical password can be used. A virtual keypad can be provided through which password can be entered and can define some special characters in the characters set for text password for graphical password we can draw images or symbols on the virtual screen and can used those images as password.

Conclusion:

We have proposed CaRP, a new security primitive relying on unsolved hard AI problems.CaRP is both a Captcha and a graphical password scheme. The notion of CaRP introduces a 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 used for every login attempt to make trials of an online guessing attack computationally independent of each other.

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] 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.

[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 TippingPoint DVLabs, 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.