RESEARCH ARTICLE OPEN ACCESS

Captcha as Graphical Password Using Carp Technique

Mr. T. Kumesh(Assistant Professor) [1] , Amala Rani. S

Department of CSE, PSN Engineering College
Tirunelveli.

----------**********----------

ABSTRACT:

In the Network Security, many security primitives are there based on hard mathematical problems. A new paradigm is emerged as an exciting one for the security using hard AI problems. In this paper we present a new security primitive based on hard AI Problems namely CaRP(Captcha as Graphical Passwords). It is a novel family of graphical password systems built on top of captcha technology. It is a graphical password scheme as well as it addresses a number of security problems such as online guessing attacks, relay attacks, shoulder surfing attacks. A CaRP also offers a novel approach to address the image hotspot problem in popular graphical password systems such as passpoints, that lead to week password choices. CaRP is not a proper solution but it offers security and usability for some practical applications for improving online security.

Keywords**:- Graphical password, password, hotspots, CaRP, Captcha, dictionary attack, password guessing attack, security primitive.**

----------**********----------

I. INTRODUCTION

Graphical passwords are knowledge-based authentication mechanisms where users enter a shared secret as evidence of their identity However, where text passwords involve alphanumeric and or special keyboard characters, the idea behind graphical passwords is to leverage human memory for visual information, with the shared secret being related to or composed of images or sketches. Despite the large number of options for authentication, text passwords remain the most common choice for many reasons. Passwords are the most common method of authenticating users, and will most likely continue to be widely used for the foreseeable future, due to their convenience and practicality for service providers and end-users. Although more secure authentication schemes have been suggested in the past. Authentication refers to the process of confirming or denying an individual's claimed identity. Authentication schemes require users to memorize the passwords and recall them during log-in time. Also, adequate authentication is the first line of defence for protecting any resource. Graphical techniques are one of the many alternatives proposed to address the weaknesses in the conventional authentication based upon username and passwords.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), also known as Human Interactive Proof (HIP), is an automated Turing test in which both generation of challenges and grading of responses are performed by computer programs. CAPTCHAs are based on Artificial Intelligence (AI) problems that cannot be solved by current computer programs or bots, but are easily solvable by humans. A client who provides a correct response to a challenge is presumed to be a human; otherwise a bot. CAPTCHAs have been widely used as a security measure to restrict access from bot. As per Bin B. Zhu present a security analysis of the representative schemes we have identified. For the schemes that remain unbroken, he present our novel attacks. For the schemes for which known attacks are available,

he propose a theoretical explanation why those schemes have failed. Next, he provide a simple but novel framework for guiding the design of robust IRCs. Then he propose an innovative IRC called Cortcha that is scalable to meet the requirements of large-scale applications. Cortcha relies on recognizing an object by exploiting its surrounding context, a task that humans can perform well but computers cannot. Cortcha's speed is not a satisfied one, and it does not have large-scale usability.

In Paul Dunphy's paper he investigate the novel idea of introducing back-ground images to the DAS scheme, where users were initially supposed to draw passwords on a blank canvas overlaid with a grid. Encouraging results from our two user studies have shown that people aided with background images tended to set significantly more complicated passwords than their counterparts using the original scheme. In this the disadvantages are shoulder-surfing and interference between multiple passwords are concerns for BDAS too. S. Wiedenbeck present Various Authentication Systemssuch as Token Based Biometric system, Knowledge based Authentication, Click-Based Graphical Password ,Persuasive Cued Click Points for resolving the main drawback the input tolerance. Norafida Bt.Ithnin propose a new usable graphical password prototype of the recognition base graphical password. In this design we will focus on the usability features of the system to give new usable graphical password system. Graphical passwords schemes are an alternative authentication method of the conventional password scheme in which users click on images to authenticate themselves rather than type the conventional passwords as letters or numbers or mixed. This usability set includes the easy of use, memorize, creation, learning and satisfaction. Moreover, this work proposes to build a new system of graphical password system that provides promising usability features. In M.Z. Jali's paper, two methods of graphical technique, namely 'click-based' and 'choice-based' are studied in term of their usability for web-based authentication. A total of 21 participants were asked to use prototype implementations and provide feedback. From the data analysed in terms of number of attempts, accuracy, time, pattern and user feedback, it was found that the choice-based method performed better. CCP addresses the 'Passpoints' problem by letting users to click once on a series of images with the current click determines the next images. In this Appropriate evaluation in terms of usability and security will then be conducted in order to validate the enhanced scheme. On the other in Philippe Golle's described an ac-curate in telling apart the images of cats and dogs used in Asirra. This classi er is a combination of support vector machine classi ers trained on color and texture features extracted from images. Asirra to be deployed in a way that maintains an appealing balance between usability and security. One contribution of our work is to inform the choice of safeguard parameters in Asirra deployments.

Several techniques have been developed that help to protect transactions performed over insecure terminals. TAN codes, security tokens, and smart cards prevent an attacker who obtained the user's password from signing transactions under the user's identity. As per Guenther Starnberger's paper, it contributes with the QR-TAN authentication technique. QR-TANs are a transaction authentication technique based on two-dimensional barcodes. Compared to other established techniques, QR-TANs show three advantages: First, QR-TANs allow the user to directly validate the content of a transaction within a trusted device. Second, validation is secure even if an attacker manages to gain full control over a user's computer. Finally, QR-TANs in combination with smart cards can also be utilized for offline transactions that do not require any server. QR-TANs allow for less costs at the service provider while at the same time providing a higher level of security. Unlike other proposed techniques, QR-TANs only require modest communication and computation capabilities at the trusted device.

Michael K. Reiter proposed the paper as evaluate new graphical password schemes that exploit features of graphical input displays to achieve better security than text- based passwords. Graphical input devices enable the user to decouple the position of

inputs from the temporal order in which those inputs occur, and we show that this decoupling can be used to generate password schemes with substantially larger (memo-rable) password spaces. In this paper we explore an approach to user authentication that generalizes the notion of a textual password and that, in many cases, improves the security of user authentication over that provided by textual passwords. We design and analyze graphical passwords, which can be input by the user to any device with a graphical input interface. They are exploring alternative schemes for modeling the memorability of DAS passwords that we hope will capture their high level structure more intuitively than our current models. The goal is to capture the concept of organized drawings, in which the view of the whole is more than just the sum of the individual parts that constitute it. V. Bhusari invented a proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumerical passwords. The selection of regions from an image can be done rather than typing characters as in alphanumeric password approaches. Graphical passwords are better alternative than the traditional alphanumeric passwords as memorization of pictures is easier than words. So other systems which we have discussed have been developed to overcome the problems of predefined regions, predictable patterns and password attacks, a new method called Cued Click Points (CCP) is a proposed as an alternative to PassPoints. In addition selection of the sound signature can be done corresponding to each click point which can be used by the user in recalling the click point on an image.

In the CCP technique the users are required to remember only one point in one image and the next image is displayed only when the user clicks on the click point of previous image correctly. A graphical password system with a supportive sound signature is much more helpful as it helps to increase the remembrance of the password and has shown very good performance.

In our proposed system, 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. A password of CaRP can be found only *probabilistically* by automatic online guessing attacks including brute force attacks, a desired security property that other graphical password schemes lack. Hotspots in CaRP images can no longer be exploited to mount automatic online guessing attacks, an inherent vulnerability in many graphical password systems. CaRP forces adversaries to resort to significantly less efficient and much more costly human-based attacks. In addition to offering protection from online guessing attacks, CaRP is also resistant to Captcha relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. CaRP can also help reduce spam emails sent from a Web email service.

II. METHODOLOGIES

A new paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. Is it possible to create any new security primitive based on hard AI problems. This is a challenging and interesting open prob-lem. In this paper, we introduce a new security primitive based on hard AI problems, namely, a novel family of graphical pass-word 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. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt.

The notion of CaRP is simple but generic. CaRP can have multiple instantiations. In theory, any Captcha scheme relying on multiple object classification can be converted to a CaRP scheme. 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. Defense against online dictionary attacks is a more subtle problem than it might appear. CaRP also offers protection against relay attacks, an increas-ing 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.

A. Graphical Passwords

A large number of graphical password schemes have been proposed. They can be classified into three categories accord-ing to the task involved in memorizing and entering passwords: recognition, recall, and cued recall. Each type will be briefly described here. More can be found in a recent review of graphical passwords

A *recognition-based* scheme requires identifying among decoys the visual objects belonging to a password portfolio. A typical scheme is Passfaces wherein 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. Story is similar to Passfaces but the images in the portfolio are ordered, and a user must identify her portfolio images in the correct order. Déjà Vu is also similar but uses a large set of computer-generated "random-art" images. Cognitive Authentication requires a user to generate a path through a panel of images as follows: starting from the top-left image, moving down if the image is in her portfolio, or right otherwise. The user identifies among decoys the row or column label that the path ends.

B. 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 recogni-tion while the latter relies on recognition of non-character objects. Security of text Captchas has been extensively studied. The following principle has been established text Captcha should rely on the difficulty of character segmenta-tion, which is computationally expensive and combinatorially hard.

Machine recognition of non-character objects is far less capable than character recognition. IRCs rely on the difficulty of object identification or classification, possibly combined with the difficulty of object segmentation. Asirra relies on binary object classification: a user is asked to identify all the cats from a panel of 12 images of cats and dogs. Security of IRCs has also been studied. Asirra was found to be susceptible to machine-learning attacks. IRCs based on binary object classification or identification of one concrete type of objects are likely insecure. Multi-label classification problems are considered much harder than binary classification problems. Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words (rather

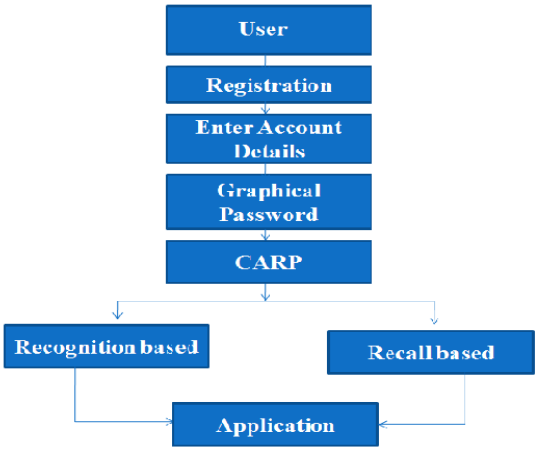
than the recommended jumble of characters).

CAPTCHA AS GRAPHICAL PASSWORDS

In CaRP, a new image is generated for every login attempt, even for the same user. CaRP uses an *alphabet* of visual objects (e.g., alphanumerical characters, similar animals) to generate a CaRP image, which is also a Captcha challenge. A major difference between CaRP images and Captcha images is that all the visual objects in the alphabet should appear in a CaRP image to allow a user to input any password but not necessarily in a Captcha image. Many Captcha schemes can be converted to CaRP schemes, as described in the next subsection.

CaRP schemes are clicked-based graphical passwords. According to the memory tasks in memorizing and enter-ing a password, CaRP schemes can be classified into two categories: recognition and a new category, *recognition-recall*, which requires recognizing an image and using the recog-nized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition and cued-recall, and retains both the recognition-based advantage of being easy for human memory and the cued-recall advantage of a large password space. Exemplary CaRP schemes of each type will be presented later.

Overall System Design



Methods:

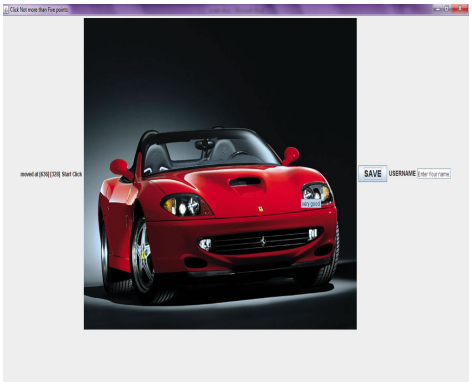


Fig a) Recognition Based

Fig b) Recall Based

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 intro-duces 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. 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, More importantly, we

expect CaRP to inspire new inventions of such AI based security primitives.

References:

- *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.*
- *(2012, Feb.). The Science Behind Passfaces [Online].Available:http://www.realuser.com /published/ScienceBehindPassfaces.pdf*
- *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.*
- *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.*
- *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 user-drawn graphical passwords," ACM Trans. Inf. Syst. Security, vol.*
- *K. Golofit, "Click passwords under investigation," in Proc. ESORICS, 2007, pp. 343–358.*
- *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.*
- *J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in Proc. USENIX Security, 2007, 103–118.*
- *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.*
- *P. C. van Oorschot and J. Thorpe, "Exploiting predictability in click-based graphical passwords," J. Comput. Security, vol. 19, no. 4, 669–702, 2011.*
- *T. Wolverton. (2002, Mar. 26). Hackers Attack eBay Accounts [Online]. Available: http://www.zdnet.co.uk/news/networking/20 02/03/ 26/hackers-attack-ebay-accounts-2107350/*
- *HP TippingPoint DVLabs, Vienna, Austria. (2010). Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs [Online]. Available: http://dvlabs.tippingpoint.com/toprisks2010*
- *B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161–170.*
- *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.*
- *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.*