International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.3, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

A HYBRID GRAPHICAL PASSWORD SECURITY SYSTEM BASED ON CAPTCHA AND DATA HIDING

SWATHI M.B[1]. SUDARSHAN K[2].

[1]M.Tech Student, Department of Computer Science & Engineering, Srinivas Institute of Technology, Mangalore, Karnataka, India

[2]Associate Professor, Department of Computer Science &Engineering, Srinivas Institute of Technology, Mangalore, Karnataka, India

Article Received: 29/04/2015

Article Revised on:04/05/2015

Article Accepted on:09/05/2015

SWATHI M.B.

ABSTRACT

Password system is a type of security system used for user authentication. It protects the confidential information or data from unauthorized access. There are many types of password security systems are available for example textual passwords, graphical passwords etc. Textual password system is the traditional security system which uses a string of characters as passwords and this security system is widely used nowadays. This textual password system provides lower level of security compared to other password systems. The main disadvantage of textual password system is that they are more vulnerable to shoulder-surfing attacks. The Graphical password system is a new type of security system which provides higher level of security. The proposed password system is called as a hybrid graphical password security system based on Captcha and data hiding where, the passwords are the Captcha images. We call this technology as CaRP (Captcha as graphical passwords). CaRP provides more security and it resolves the problem of online guessing attacks, relay attacks etc. Data hiding is the method used to hide the confidential data where any sensitive data can be hidden inside an image or image can be hidden inside another image.

Keywords— CaRP; Graphical passwords; Captcha; Shoulder Surfing attacks; Dictionary attacks; Relay attacks.

INTRODUCTION

The security system is very important to secure the confidential data or information. There are many number of security algorithms which are available such as cryptographic algorithms etc. These cryptographic algorithms are divided into public key cryptography and private key cryptography. Artificial Intelligence is the new primitive used for security. Captcha system is one of the important primitive which comes under this Artificial Intelligence. In this Captcha system, the user is presented with the challenge for example a puzzle, and the user has to resolve the challenge in order to authenticate.

Traditional password scheme uses textual passwords or alphanumerical characters and this password scheme is easy but the problem is that, if the user provide small password then the hacker can easily guess the password. These small passwords can be hacked easily by different hackers. The textual passwords with greater length are hard to remember and if the passwords are not frequently used then the passwords can be easily be forgotten.

The proposed system is called as the hybrid graphical password security system based on Captcha and data hiding. The graphical passwords [1] are alternative to the textual passwords, where graphical password system uses pictures or images as passwords instead of alphanumerical passwords. The images used here are called as the Captcha image. This technology is hence called by the name CaRP (Captcha as graphical passwords). The graphical based password system is the combination of both recognition and recall based techniques where in the recognition method the user has to identify the images or objects which are displayed to him/her and in the recall based method the user has to recall the images which he/she had already selected.

The proposed system is based on the click-method where the users are likely to select the portions of the image as clickpoints. Data hiding is the method used to hide the confidential data where any sensitive data can be hidden inside an image or image can be hidden inside another image. This hybrid graphical password system includes two phases a registration phase and a login phase. During the registration phase, the user has to select his/her profile photo and then select an image which he/she wants to hide inside the Captcha image this is called data hiding. The user enters the key to hide the image. A set of Captcha images are displayed to the user and the user has to click on some portions of the image. During the login process, the user has to click the exact portions on the image. If the user clicks the exact points on the image as he/she done in the registration phase then he/she is the authenticated user to use the account. Key is provided again by the user and the hidden image or data can be viewed by providing the key. The user has to enter the same key which he/she is already entered during the registration phase. CaRP image is generated for every login attempt. CaRP offers protection against online dictionary attacks, relay attacks.

BACKGROUND AND RELATED WORK

Graphical passwords

Graphical passwords are alternatives to textual passwords where pictures, images are used as passwords. There are many number of graphical password systems have been proposed. This graphical password security scheme is classified into four categories:Recognition based system, pure recall based system, cued recall based system and hybrid system.

The recognition based system involves identifying whether the user has seen the image before and the user has to identify the previously seen images. One of the example for recognition based system is passfaces [2]. In the pure recall based system the user has to recall the images he/she had selected before in the registration phase. In the cued based system the user is provided with the hint so that the user can recall his/her password which he/she has selected before. The hybrid system is the combination of one or more schemes such as recognition and pure recall based or text and graphical password system. Example for the graphical password scheme is passpoints [3]. In the passpoint scheme the password is derived from the sequence of click points on the image and the user may select any pixel on the image as click points as his/her password.

Captcha and captcha authentication

Captcha is used to solve the AI problems [4]. Captcha is divided into two types: Text Captcha and image recognition Captcha. The textcaptcha rely on the character segmentation. Both Captcha and password in a user authentication protocol is introduced in [5]. We call Captcha based password authentication as (CbPA) protocol. This is mainly used for online dictionary attacks. The CbPA protocol includes solving a Captcha challenge after providing a valid pair of userID and password. If userID and password is found to be invalid then the user is provided with a Captcha and he/she has to solve the Captcha challenge before being deneid access.

Data hiding

Data hiding is the important method used to hide the confidential data by securing the data where the data can be hidden inside an image. The data can be a document or an image. In this paper an image is selected during the registration phase that the user wants to hide inside the Captcha image. Key is provided by the user to hide the selected image and the user has to reenter the key to view the hidden image. Steganography [6] is the technique used for hiding the data. It provides better security compared to cryptography. Here the original data is hidden within the carrier. The carrier can be image or audio. An image can be hidden inside another image using variable rate steganography. The images used may be color or other images.

Captcha as Graphical password(CaRP)

One of the common attacks on the password is the guessing attack. To solve this problem the graphical passwords are introduced which provides larger password space compared to the textual passwords and it makes the passwords harder to guess. CaRP schemes are click-based graphical passwords. CaRP provides security for the channels between the client and server. There are two types of CaRP schemes: Recognition based CaRP and Recall based CaRP. ClickText, ClickAnimal are the examples for recognition based CaRP where clickText is based on the text Captcha which consists of visually confusing characters. This clickText is the sequence of characters in the alphabet and generated by the Captcha engine. ClickAnimal is based on the CaptchaZoo [7]. A CaptchaZoo uses 3D models of horse and dog with different colors, poses etc. Recognition-Recall CaRP is a CaRP scheme where a password is the sequence of points on the image.

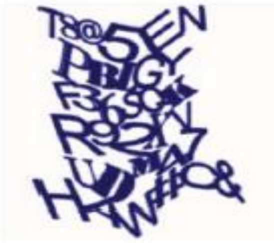

Fig.1. A Clicktext image

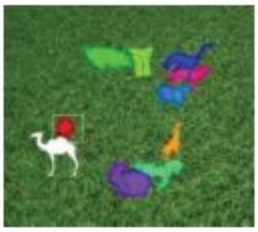

Fig.2. A Clickanimal image

Proposed method

We present a new security primitive based on hard AI problems, a novel family of graphical password systems built on top of Captcha technology and Data Hiding, 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 such as online guessing attacks, relay attacks, and shoulder-surfing attacks. 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 ad- dress the well-known image hotspot problem in popular graphical password systems, such as PassPoints, that often leads to weak password choices. CaRP is fit well with some practical applications for improving online security. We present exemplary CaRPs built on both text Captcha and image-recognition Captcha. CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. We have also implemented data hiding concept where the data can be hidden inside the Captcha image and we provide key to that image. We can extract the hidden image by entering the key. We also implemented one application where we can upload some documents and security is provided with the Captcha image and we can download the document by providing the clickpoints on that Captcha image.

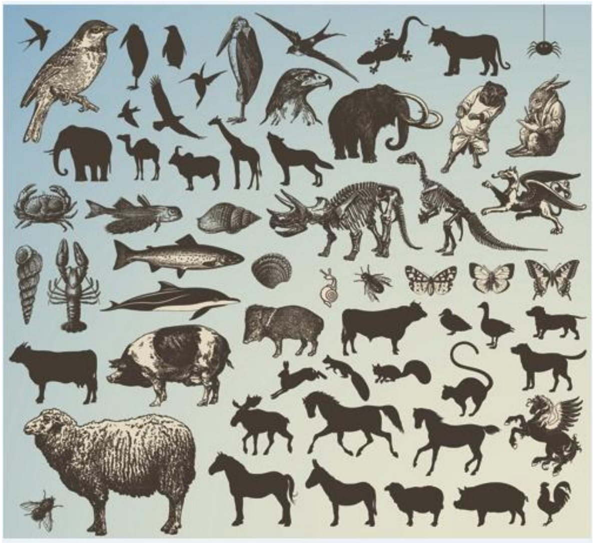

Fig.3. Captcha image set

Security of Underlying captcha

CaRP doesnot depend on any specific type of the Captcha scheme. If one Captcha scheme is broken, then a new type of Captcha scheme may appear. Captcha password scheme is more secure compared to textual password scheme which is resistent to shoulder surfing attack. In this Captcha scheme user need to click on the exact positions or points on the image. So it is difficult for the hacker to hack the captcha image.

CONCLUSION

This proposed method is a new security primitive on unsolved hard AI problem. CaRP is the combination of both Captcha and a graphical password scheme. This CaRP introduces a new family of graphical password. The proposed method is called as a hybrid graphical password security system because it includes both Captcha and data hiding method.

REFERENCES

[1]. Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang, School of Computer Science, A Graphical Password Based System for Small Mobile Devices University of Jazan,PoBox 114, Kingdom of Saudi Arabia.

[2]. Hai tao, Pass-Go, a New Graphical Password Scheme, Master Thesis University of Ottawa Canada, June 2006.

[3]. S.Wiedenbeck, J. Waters, J. C.Birget, A. Brodskiy, and N. Menon, PassPoints:Design and longitudinal evaluation of a graphical password system, Int. J. HCI, vol. 63, pp. 102 127, Jul. 2005.

[4]. M. L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, CAPTCHA: Using hard AI problems for security, in Proc .Eurocrypt, 2003, pp 294311.

[5]. B. Pinkas and T. Sander, “Securing passwords against, dictionary attacks,” in *Proc. ACM CCS*, 2002, pp. 161–170.

[6]. Aravind kumar, International journal of computer applications, voulume 9, no.7, November 2010

[7]. 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, pp. 3–8.