IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 3, March 2015.
www.ijiset.com
ISSN 2348 – 7968

A Text and Image Recognition CAPTCHA- A Cognitive Authentication Schemes Based On Hard AI Problems

Kavitha Balan[1], Ranjani Ramasamy[2]

[1]Computer Science and Engineering, IFET College of Engineering,

Villupuram-605 108, India.

[2]Computer Science and Engineering, IFET College of Engineering,

Villupuram-605 108, India.

Abstract

Secure Computing refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Several existing techniques based on hard mathematical problems such as RSA public-key cryptosystem, Rabin encryption, Diffie-Hellman key exchange, EIGamal encryption have a limitations is unsecure and limited success. In order to tackle these challenges, a captcha and a graphical password schemes is addressed. Captcha and a gRaphical Password (CaRP) is a click-based image authentication graphical password, where a sequence of clicks on image is used to derive a password. CaRP offers a protection against relay attacks, an increasing threat to bypass captcha protection and also protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. Advantage of proposed captcha is to prevent botnet and spam attacks.

Keywords: Cognitive authentication, click points graphical password.

1. Introduction

Secure Computing refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most secure computing measures involve data encryption and passwords. A password is a secret word or phrase that gives a user access to a particular program or system to provide security [2].CAPTCHA as click based graphical passwords image based Authentication (IBA) is based on user's successful identification of his image key password. After the username is sent to the authentication process, it responds by displaying an image which consists of click points on the image to set the user's password. The purpose of this paper is to present the authentication process which is more secure the downloading and uploading the secure files [3]. The usage of the graphical password is by recognizing the images that comprise it from among many more images. This image password can be of any person, nature, flower or any blur image. In this password scheme, a user is asked for her user name and password i.e. graphical password. The user must correctly click the position like hotspots on the image to set as a password [4].

2. Benefits of secure computing

- Protect yourself - Civil liability: You may hold liable to compensate a third party should they experience financial damage or some distress as a result of their personal data being stolen from you or leaked by you legally.
- Protect your credibility - Compliance: You may require some compliancy with the some acts such as Data Protection Act, the FSA, SOX or some other regulatory standards. Each of these substances stipulates that certain measures to be taken to protect the data from your network system.
- Protect your reputation – Spam: Some common use for infected systems is come front to join them to a botnet which is a collection of infected machines which takes orders from a command server and use them to send out some spam emails. This spam emails can be traced back by you, your server could be

ISSN 2348 – 7968

saved as blacklisted and you could not be able to send email.

- Protect your income - Competitive advantage: There are a number of "hackers-for-hire" advertising their services on the internet by means of selling their skills in breaking into company's servers to stolen some authorized one such as client databases, proprietary software, and merger and acquisition information, personnel detail set.
- Protect your business – Blackmail: A seldom-reported source of income for "hackers" is to broken into your server, change all your passwords and lock your account details. The password is then sold back to you. Note that the "hackers" may implant a backdoor program on your server so that they can repeat the exercise during any time.
- Protect your investment - Free storage: Your server's hard drive space is used or sold on to house the hacker's video clips, music collections. Your server or computer will becomes continuously slow and your internet connection speeds low or deteriorate due to the number of people connecting to your server in order to download some of the offered wares.

3. Applications of CAPTCHA

There are number of applications of CAPTCHA on the web which are defined as follows.

1) Registering the web forms

There are many sites on the Internet which provide free registration to avail their services. But they are having the choice to web bots. It may come into the form of scripts which can register thousands of email accounts on the internet, thus leads to wasting the space of web[5].

2) Online polling sites

These sites take user's response or feedback in the form of question type. To ensure that only human makes the response they make use of CAPTCHA[5].

3) To avoid web crawling

If a site doesn't want to get indexed by a search engine then they can make use of CAPTCHA[5].

4) E-Ticketing[5]

5) Preventing Dictionary Attacks and E-mail spam

It is a type of attack in which the intruder trying to determine the password by searching a large no of possibilities. It is different from Brute Force Attack in which all possibilities are searched[5].

4. Classification of CAPTCHA

CAPTHCAs means presenting a challenge response test to the users or humans. Some types of CAPTCHAs are:

1. CAPTCHAs based on text

In text based captcha the number of classes of some alphanumeric are very small so the problems occur for user to identify the correct alphanumeric characters. The text based captcha is possible to identify the alphanumeric through Optical character recognition (OCR) technique [6].

2. CAPTCHAs based on image

In image based CAPTCHAs user work is to identity image. The pros of image based CAPTCHA is that pattern can be recognized based on the test and therefore it is difficult to break this test using this pattern recognition technique [6].

3. CAPTCHAs based on audio

Audio-based CAPTCHAs are truly based on particularly the sound-based systems. These type of CAPTCHAs are developed for visually disabled users. In this type of CAPTCHA, first the user wants to listen to the audio and after that submits the word that was spoken.The audio-based system is based on the difference in the ability between computer machines and humans in recognizing spoken language [6]. The distorted sound clip contains some spoken word and then presented to the user to enter the right alphanumeric characters. The user must ask to enter exactly the same words as spoken inthe audio clip.

4. CAPTCHAs based on video

Video CAPTCHA is used by lesser amount of people. In video-based CAPTCHAs, three forms of words

ISSN 2348 – 7968

(tags) are provided to the user that describes a video clip. Only the test passed if the user's tag must match to a set of automatically generated ground truth tags. [6].

5. CAPTCHAs based on puzzle

Usually in puzzle based CAPTCHA a given picture is divided to chunks. A user is supposed to combine these chunks so as to form the complete picture same as the original one [6].

5. Proposed Work

➢ In this paper, the author presented a authentication based passwords, a novel family of graphical password systems built on top of Captcha technology, which we callclick based Captcha as graphical passwords (CaRP).

➢ CaRP is both a Captcha and a graphical password scheme which is based fully on click based image authentication. CaRP addresses a number of security problems, such as online guessing attacks, brute force attacks and dual-view technologies, shoulder-surfing attacks.

6. System Architecture

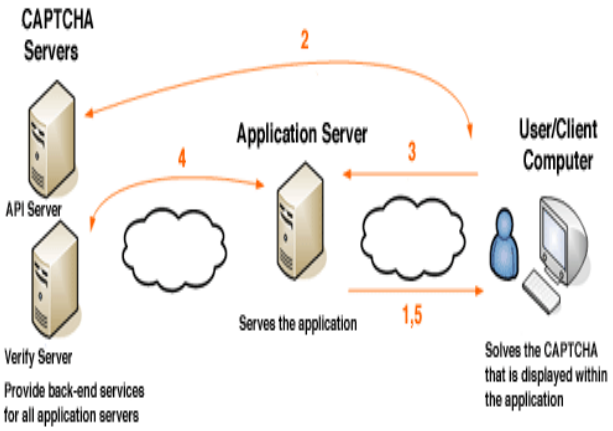

Fig 1. Proposed CAPTCHA

The above diagram explains that

1) Application server provides the application thatthe user wants.

2) CAPTCHA server provides click based image as a CAPTCHA and then send into the user/client computer.

3) After provided the CAPTCHA the user will solve the CAPTCHA that is displayed within the application.

4) After solving the CAPTCHA, the application server will verify the CAPTCHA by using API server and also it provides back-end services for all application servers.

5) After verified the application server will provide the application. (Fig, 1)

7. Related Works:

1. Securing passwords against dictionary attacks

The use of passwords is a major important point of vulnerability in computer security. Passwords are often easy to guess by using some automated programs running to find dictionary attacks. Passwords isthe most commonly used for authentication. From the perspective of a service provider this problem needs to be solved within real-world constraints such as the available hardware and software platforms. From a user's point of view user-friendliness is a important. In this paper the author suggested that a novel authentication scheme that preserves the advantages of conventional password authentication process, and also simultaneously raising the costs of online dictionary attacks by orders of magnitude. The proposed scheme was easily implemented and overcomes some of the difficulties of previously suggested methods of improving the security of user authentication schemes. Our key idea was 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 can be done without affecting the usability of the system. The proposed scheme provides some better protection against denial of service attacks against user accounts.

2. Techniques used in graphical passwords

ISSN 2348 – 7968

2.1)Recognition-Based Technique:

In recognition based technique, users will select pictures, logos or any symbols from already stored image. For authentication process user wants to recognize the image, and then he choose as a password [7].

2.2)Recall-Based Technique:

In these types of technique, there are two types. They are

1) Pure Recall Based.
2) Cued-Recall Based.

2.2.1)Pure Recall based:

In this type, a user itself generates his or her password without applying any clue or hint [7].

2.2.2) Cued-Recall Based:

In the cued-recall based technique, the image is given as the clue or hint to the user. For example, to click a set of option means a set of point on an image provide as a hint that will help the user to recall their passwords [7].

Types:

- Pass points

In this technique image is not secret and has no option to the user to remember their click point by passing in to next click on image.

- PASSMAP

In this technique we can use a password as a landmark on a known place journey. This is very common technique to use image based password to secure the personnel documents and protect the database and any type of accounts [7].

3. Cognitive authentication schemes safe against spyware

The author's previous work was taken advantage of the vast capacity of human memory to design protocols that use each memory item only once, and are therefore as safe against eavesdropping as one time passwords. Here the author proposed a challenge response protocol, where authentication is based on the user answering correctly a sequence of challenges posed by the computer. The challenges (or queries) are based on a shared secret between the computer and the user, which consists of a random division of a fixed set ofpictures into two sub-groups. Authentication was done via a challenge-response protocol: the computer poses a sequence of challenges to the user, which can only be answered correctly by someone who knows the shared secret. Once the probability of random guessing goes below a fixed threshold, the computer authenticates the user [8].

8. Conclusion

The author concluded thata authentication based passwords, a novel family of graphical password systems built on top of Captcha technology, which we call click basedCaptcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme which is based fully on click based image authentication.CaRP addresses a number of security problems, such as online guessing attacks, brute force attacks and dual-view technologies, shoulder-surfing attacks.A new CaRP image, which is also a CAPTCHA based challenges, is used for every login attempt to make trials of an online guessing attack. CaRP can also used to reduce spam emails sent from a Web email service. Like CAPTCHA, click based CaRP utilizes unsolved AI problems.

9. References

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, 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.

[2]http.//www.wikipedia.com/computer security

[3] Mr. A. A. Shinde*, Ms. S.R. Chokhandre, Mrs. R.C. Roychaudhary, Mrs. S. S. Telrandhe Mrs. C. N. Rokde*Information Technology & RTMNU India* " A Survey: Login with Image Based Password Authentication" , Volume 4, Issue 3, March 2014

[4] Navnath D. Kale, Megha M. Nalgirkar"An Ample-Range Survey on Recall-Based
Graphical Password Authentication Based On Multi-Line Grid and Attack Patterns",International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-5, April 2013

[5] Baljit Singh Saini, 2Anju Bala *Asst. Professor, Deptt. CSE/IT, Research Scholar Lovely Professional University (Punjab), INDIA Lovely Professional University (Punjab), INDIA* "A Review of Bot

ISSN 2348 – 7968

Protection using CAPTCHA for Web Security", *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 8, Issue 6 (Jan. - Feb. 2013), PP 36-42 www.iosrjournals.org*

[6] Ved Prakash Singh, Preet Pal School of Computer Science, Lovely Professional University Phagwara, Punjab "Survey of Different Types of CAPTCHA", Ved Prakash Singh et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2242-2245

[7] Navnath D. Kale, Megha M. Nalgirkar "An Ample-Range Survey on Recall-Based Graphical Password Authentication Based On Multi-Line Grid and Attack Patterns" International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-5, April 2013

[8] Daphna Weinshall School of Computer Science and Engineering The Hebrew University of Jerusalem, Jerusalem Israel 91904, daphna@cs.huji.ac.il "Cognitive Authentication Schemes Safe Against Spyware", In Proc. IEEE Symposium on Security and Privacy (S&P), May 2006.