ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Literature Survey on Data Security using Carp Two Step Authentication based on Human and Hard AI Problems

R.G.Vetrivel[1], J.Vasanth Kishore[2], B. Arun Kumar[3], S.Thivaharan[4]

B.Tech Student, Department of IT, Kalaignar Karunanidhi Institute of Technology, Tamilnadu, India[1,2,3]

Assistant Professor, Department of IT, Kalaignar Karunanidhi Institute of Technology, Tamilnadu, India[4]

Abstract: This paper introduces image based CAPTCHA to protect user data or unauthorized access of information. Here the password is created from images and text password. The Current system is based on only text password but it has some disadvantages like small password mostly used and easy to remember. This type of password is easy to guess through different attack i.e. dictionary attack and brute force attack. We are proposing a new system which uses multiple servers, enabling added level of security to the existing authentication, thereby providing access to the database. As this is a technique based on recognition of graphical background more security is achieved as well as easy to remember.

Keywords: CAPTCHA, Password, dictionary attack, brute force attack, graphical password, multiple server.

INTRODUCTION

Security is most important in our daily life. CAPTCHA standing for "Completely Automated Public Turing test to tell Computers and Humans Apart" is an automatic challenge-response test to distinguish between humans and machines. CAPTCHA is used for protection against different attack. In image based CAPTCHA is click based graphical passwords, where sequence of clicks on an image is used to derive a password. It provides protection against online dictionary attacks on password. For login every time click on images and type password. CAPTCHA can be applied on touch screen devices where on typing passwords is not more secure, especially for secure internet applications such as e-banks. In early system only text password is used which is very difficult to remember if enter a long password. If we use smaller password then it can be easily identify and we also use common password for many accounts so for that Image based CAPTCHA provide more security during authentication.

LITERATURE SURVEY

[1]MERGING CAPTCHA AND GRAPHICAL PASSWORD ON NP HARD PROBLEMS IN AI: NEW SECURITY ENHANCING TECHNIQUE

In this paper the author explained about the CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) which is a test build by computer programs which human can pass but computer programs cannot pass.

A new technology is built over the CAPTCHA called graphical CAPTCHA which is resilient to dictionary attack and hence more secure with the hybrid use of CAPTCHA and graphical password one can address a number of security problems such as relay attacks, CARP does not act as a cure all technique but it stipulates security and usability to legitimate use in real time applications.

[2]TOWARDS NEW SECURITY PRIMITIVES BASED ON HARD AI PROBLEMS

The paper consists of hard mathematical problems used to convert the CAPTCHA into graphical password system. Using hard AI problems for security leads to an emerging new paradigm. This paradigm has achieved just a limited success. It has many unexplored areas. This paper is motivated to a new security primitive based on hard AI problems.

[3]BREAKING E-BANKING CAPTCHAS

This paper shows that many financial institutions have developed CAPTCHA to perfect their services. Example e-banking .it provides automated attacks and uses CAPTCHA for their logins. CAPTCHA provide security for e-banking transactions by man in middle (MIM) attacks. Despite of financial risk, Security of e-banking CAPTCHAs is largely unexplored. In this paper we report the first comprehension study on e-banking. They also show essential difficulties of designing e-banking CAPTCHAs as both unusable and secure.

[4]PROBABILISTIC MODEL CHECKING OF CAPTCHA ADMISSION CONTROL FOR DOS RESISTANT ANTI-SPIT PROTECTION

In this paper the Voice over IP (VoIP) services is expected to play a key role to new ways of communication. It takes advantage of IP by using packet networks to transmit voice and multimedia data thus providing extreme cost savings. SPAM over Internet Telephony (SPIT). A well established method to tackle due to their excessive demands for bandwidth. We qualifies the cost and the benefits in bandwidth usage through probability model checking for different admission control, we conclude with the comments on how appropriate is each policy in tackling Dos attacks.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

[5]CAPTCHA DESIGN: COLOR, USABILITY, AND SECURITY

In this paper, most users interface user's color which can greatly enhance their design, because the use of color is typically a usability issue it rarely causes security failures. How they are using colors when designing CAPTCHAs a standard security tech that many commercial websites apply widely can have an impact on usability and interesting but critical implications for security the author examine some CAPTCHA to determine where their use of color negativity affects their usability, security or both.

[6]SECURING PASSWORDS AGAINST DICTIONARY ATTACKS

In this paper the author mentioned about the use of password is a major point of vulnerability in computer security password are often case to guess by automated programs password is used as mostly for the authentication the user authentication is clearly a practical problem. This problem needs to solve within real world constraints such as available hardware & software infrastructures. In this the user friendliness is also a key requirement. In this paper they suggest a novel authentication scheme. If preserves the advantages of conventional password authentication. Their key idea is to efficiently combine traditional password authentication with a challenger that is very easy to answer by human users. But it wants to be in feasible for automated programs to run dictionary attacks. If done without affecting the usability of system.

[7]DISTORTION ESTIMATION TECHNIQUES IN SOLVING VISUAL CAPTCHAS

The paper described two distortion estimation techniques for object recognition that solve two visual CAPTCHA ("Completely Automated Public Turing Test to tell Computer and Human Apart") with the high degree of success. They have developed a correlation algorithm that collect identifies the word in an EZ-Gimpy challenge image 99% of the time and a direct distortion estimation algorithm that correctly identifies the four letters in a Gimpy-r challenge image 78% of the time.

[8]MACHINE LEARNING ATTACKS AGAINST THE ASIRRA CAPTCHA

In this paper, it relies on the problem of distinguishing image of cats & dogs [a task that humans are very good at] these security is based on classifying these images automatically. They describe a classifier which is 82.7% accurate in telling apart the image of cats and dogs used in asirra this classifier is trained on color and texture features extracted from images. This classifier allows us to solve a 12 image asirra challenge automatically with the probability 10.3%. The probability of success is significantly then the estimate of 0.2% given for machine vision attacks. Their result suggests caution against deploying asirra without safe guards.

[9]DO BACKGROUND IMAGES IMPROVE 'DRAW A SECRET' GRAPHICAL PASSWORDS

In this paper the author said that draw a secret (DAS) is a representative graphical password scheme. If supports an overall password scheme. Revert research suggest that DAS users tends to choose week password render this theoretically sound scheme less secure in real life they investigate the novel idea of introducing background images to the DAS scheme the password on a blank canvas over lied with a grid .by drawing like this people. A set a complex password using this scheme. If reduce the chance of predictability in DAS. In this if a positive effect was observed with respect to the removability of the more complex password encouraged by the background images.

[10]PASS-GO: A PROPOSAL TO IMPROVE THE USABILITY OF GRAPHICAL PASSWORDS

The Pass Go graphical password scheme was an inspired design of an old Chinese game, Go. Here the users select the intersections on a grid as a way to input the password. It offers an extremely large full password space (256 bits for the most basic schemes). It provides acceptable usability. The largest user study involves 167 subjects on graphical passwords. It supports most application environment and input devices rather than being limited to small mobile devices (PDA) and it can be used to derive cryptographic keys.

EXISTING SYSTEM

In the existing system 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. 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.

PROPOSED SYSTEM

In our proposed we introduces image based CAPTCHA to protect user data or unauthorized access of information. In that password is created from images and text password. Current system is based on only text password but it has disadvantages small password mostly used and easy to remember. This type of password is easy to guess through

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

different attack i.e. dictionary attack and brute force attack. So we introduce the new image password scheme. In this Recognition based technique is used with numerical password which provides more security and easy to remember text and graphical password which uses multiple servers, enabling added level of security to the existing authentication, thereby providing access to the database.

CONCLUSION

This paper presents a survey on various techniques and algorithms that was proposed earlier by researchers for the better privacy-preserving data access. Our graphical password system provides more security to data and protection against different attacks. In future the scheme may be extended as a web service so that any interconnected user of the network can utilize it to the maximum without the need to implement the code.

ACKNOWLEDGEMENT

Reaching destination is not possible without a walk towards it. Of course yes, I would like to thank few people at this moment, which had been a great support for us to achieve it. With a start we would like to thank god and also we wish to thank Pongalur N Palanichamy, Founder Chairman, Mrs. Indhu Murugesan, Managing Trustee, Mr. N Anbalagan, Director, Mr. Mohandas Gandhi, Principal for their immense supervision providing all helpful needs for bringing this journal paper a successive completion. We also would like to thanks all the reference authors for the completion of this paper and we would like to thank our guide Mr.Thivaharan, Assistant Professor, Kalaignar Karunanidhi Institute of Technology.

REFERENCES

[1] Nayan Gawande," Merging CAPTCHA and Graphical Password on NP Hard Problems in AI: New Security Enhancing Technique", International Journal of Science and Research (IJSR) 3.358 Volume 3 Issue 12, December 2014.

[2] Bin B. Zhu1 and Jeff Yan2, "Towards New Security Primitives Based on Hard AI Problems",1 Microsoft Research Asia, Beijing, China, 2 School of Computing Science, Newcastle University, UK

[3] S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, "Breaking e-banking CAPTCHAs," in *Proc. ACSAC*, 2010, pp. 1–10.

[4] Emmanouela Stachtiari,Yannis Soupionis,Panagiotis Katsaros,Anakreontas Mentis,Dimitris Gritzalis, "Probabilistic Model Checking of CAPTCHA Admission Control for DoS Resistant Anti-SPIT Protection" , springer_2013 Volume 7722, 2013, pp 143-154.

[5] Ahmad Salah El Ahmad Newcastle University,UK Jeff Yan Newcastle University,UK Wai-Yin Ng Chinese University of Hong Kong ,"CAPTCHA Design: Color, Usability, and Security", IEEE Internet Computing archive Volume 16 Issue 2, March 2012 Pages 44-51 IEEE Educational Activities Department Piscataway, NJ, USA

[6] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161–170.

[7] G. Moy, N. Jones, C. Harkless, and R. Potter, "Distortion estimation techniques in solving visual CAPTCHAs," in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., Jul. 2004, pp. 23–28.

[8] P. Golle, "Machine learning attacks against the Asirra CAPTCHA," in Proc. ACM CCS, 2008, pp. 535–542.

[9] P. Dunphy and J. Yan, "Do background images improve 'Draw a Secret' graphical passwords," in Proc. ACM CCS, 2007, pp. 1–12.

[10] 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.