ISSN: 2348-2079

FEB-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

CAPTCHA AS A GRAPHICAL PASSWORD –MULTILEVEL SECURITY PRIMITIVE

Sharanya.P[1], Vijaya Sharon.A[1], Vijay.S[1], Dhivya.P[2]

ABSTRACT

Security plays an important role in all field nowadays, based on a hard AI problem for security is emerging as an new paradigm, but has been under explored the existing methodology which addresses this problem is captcha technology, But in this paper new system called captcha as graphical password along with this technology multilevel access authentication is also included that provides more security. This combined technology addresses a number of security problem such as, online guessing attack, relay attack, surfing attack etc, CaRP offers reasonable security that appears to fit well with all sort online security and provides efficient security.

I. INTRODUCTION

Image processing is a form of signal processing. An image is given as input (i.e) photography and their final outcome is parameters that are related with that image. Hence information related with the input image is generated. Optical image processing technique is used with that of Captcha Technology.

The data found in third party sites are not much secured .There is need to provide high security. Whatever high sort of security is provided it gets attached by various methods of attacks. Many problems with login attack occurs due to two main strategies,

1) denial-of-service attacks which leads to high cost and becomes highly expensive due to reactivation

2) Global password attack where it gets broken into many accounts rather to be single one. The main advantage included is avoidance of trigger

Thus frequent updating is provided to have a developed security. In encryption method is used the data to provide high security that is encrypted and decrypted when it is used. A user is able to decrypt the data with the help of private/public key. The ever-increasing growth of hackers hard AI people an security primitives was initially proposed is that cryptographic primitives that are based on hard mathematical problems that are intractable and many algorithm are also proposed with cryptography primitive.

The security is initially proposed with Captcha technology using hard AI problems. Captcha distinguishes human users form computers by presenting a challenge. This Captcha mainly provides high security then cryptographic technology. Captcha provide high online security and all online services can be performed with and maximum security can be achieved. Captcha technology provides a click based graphical password, image used CaRP are newly generated image that are generated at every authentication process.

CaRP technology provides highly multiple authentications. This multiple level login attempt helps to provide cyber security against dictionary attacks and risk attacks.

Address for Correspondence:

[1]UG, Final year Computer Science And Engineering, SNS College of Technology, TN, India. E-mail:prisy.sharon@gmail.com, dhivyasnsce@gmail.com

[2]Assistant Professor, Department of Computer Science and Engineering, SNS College of Technology, TN, India

CaRP is mainly applied and implemented on touch screen devices where on graphical password is drawn and random Captcha are generated main application of CaRP technology is implemented in e-banking users are provided with separate user name and password as first authentication step is provide. This Captcha provides a security form e-mail spammers and also reduce spamming traffic occurs using Captcha.

II. RELATED WORK

As more sensitive data is shared and stored on the internet, there will be a need for encrypted data main drawback of encrypting data is that it can be selectively shared only at coarse grained level. Where this is a fundamental security task is said to create cryptographic primitives that are based on hard AI problem. Cryptographic primitives are computational and encryption and decryption are the main two steps involved in case of this primitive process. The most notable method invented is captcha that mainly distinguishes human from machine by presenting a challenge.

A. Captcha

Captcha a new innovative primitive of providing an efficient security for online processing i.e. e-banking, its mainly based on hard AI problem .main two categories of captcha are: Text captcha and Image captcha. Compared to human recognition of a non-character object is highly hard for machine thus captcha is the best method for online security. This text captcha mainly depends on segmentation of characters .random characters are identified and entered for authentication purpose. Muti-lables the major problem found and this is much harder.

B.Graphical password

Different types of graphical password schemes has been developed and proposed, main categories are, each types are briefly explained below,

A recognition- based this is mainly done with the recognition that are done at the spot. With the spot identification we create an authentication key for the particular process for which security is provided randomly to make a successful login there must be a correct selection at each time of login

A recall based method of authentication technique that needs the user to regenerate the same result that occurred with cueing. A secret 2D grid is drawn .that user grid password provides one of the security and improves DAS's usability.

In case of cued –recall, an outer layer cue has been provided to help memorize and a password is entered this method is mainly click based process this is same as pass point but main difference is it uses one image per click next is selected deterministically.

Example of graphical password

SECURITY ANALYSIS

A. security of underlying captcha

Recognizing object in CaRP images is fundamental to CaRP. Normally captcha analyses security as one by one process or an approximate process, object segmentation is found to be a highly expensive and hard problem. upon which modern text captcha rely, A is exponentially depend on the number Z object contained polynomial depend on size x captcha :$A=\beta P(x)$where $\beta>1$ is a parameter() is a polynomial function ordinary captcha generally includes 5 to 10 characters, whereas a CaRP image typically contains 40 or more number of characters. Complexity to break click text image is highly hard. CaRP image is of two dimensional segmentation one more segmentation is not preferred, as a result distortion gets reduced in click text images to increase the usability and maintains the security level

CaRP does not rely only on one specific scheme of captcha, if any of the used schema gets deleted or destroyed it goes to next schema and construct their process. Captcha is given as or assumed as chosen pixel attack.

B. Automatic online guessing attack automatic trial and error process is executed whereas manually dictionaries can be constructed. If some probabilities are eliminated CaRP with CPA-captcha has following properties

1. Object points on a CaRP image do not be dependent on another image. especially, clickable points should also be independent on each other

2. Trials in guessing attack are found to be interdependent.

Property one is followed with a contradiction, assume there found an internal object point A on an image α that is non-negligible of object C on an image β.dependency can be exploited with a chosen pixel image α and β learn from their contained objects this experiment gives success probability.

Second property is an absolute continuation of first, where since first property internal object-points are independent so that in same way background points and boundary points are also independent of each objects because it might lead to authentication failure.

C .Relay Attacks

Relay attacks involves multiple ways of execution. Captcha technology is involved mainly in the sites were frequent surfing process is involved and also the sites need high security for the data to protect it from other attacks. Many CBPA-protocols has been compared to avoid all other new attacks that occurs to online data image used in CaRP and many tasks that are performed are found to be completely different in attack mechanism. An input is entered by captcha task on CaRP image to have level security. The total cost to solve an 1000 captcha challenges cost that occurs to break a 26-bit password

III.PROPOSED WORK

Newly proposed work comes with a idea to mainly overcome the attacks and all possible disadvantages are corrected. This system deals with achieving high probable success as compared with cryptography primitives based on hard mathematical problem and this mainly involves the role of encryption and decryption of data .this is the fundamental security task this does not gives. Appreciable security level attacked by machines easily overcome hard AI problem captcha technology was invented and used their main drawback is single level. and hence to overcome all these disadvantage ,CaRP methods used as an emerging new primitive

In Carp (captcha as graphical password) it provides multilevel authentication capabilities it includes captcha and also graphical password methodology it can solve hard AI problem easily artificial robots and all machine might find hard to find this CaRP password when compared with human users .it is an click-based and location base events hence if the location gets matched in a simple way with the entered password then it get an easy authentication .setup is also made if it matches. and provides security. This Carp has both text captcha and image-recognition password online guessing attack is the only major issues of this process hence object-point are found to be independent.

In case of this Carp technology to overcome all other problems we include multiple level authentication this online protection is implemented in e-banking application, were every user is provided with separate login page as usual. whereas that simple login password are easily hacked so as to overcome, we specify an separate account initial step we enter own password and user id as old process next user draw their preferred graphical password that remains constant .and random captcha is generated and entered .and next level is the knowledge based authentication is found as a final process .user create their own account with these password and during every authentication these steps are followed for high security.

CONCLUSION:

Newly proposed CaRP is developed with high security a primitive that mainly relies on unsolved hard AI problem. CaRP method is both the combination of captcha and graphical password and multiple authentications and implemented this new method which overcomes the online guessing attack. A CaRP image is used with captcha challenge in every login attempt .In addition ,it is found resistant to relay attacks and also it includes dual-view technologies such as shoulder –surfing is avoided .It is mainly involved to overcome from e-mail spammers that are sent from web e-mail service.

This captcha technology with CaRP method involves high security process .A newly found methodology protects mainly all online data. This CaRP had major advantage is that it does not depend on particular captcha scheme alone .If captcha gets crashed it deals with newly developed captcha scheme, we expect much more new improvements might also be developed based with AI based security primitives

V.REFERENCES

[1]. Ashwin Swaminathan, Student Member, IEEE, Yinian Mao, Student Member, IEEE, and Min Wu, Member “Robust and Secure Image Hashing”,in proc,IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 1, NO. 2, JUNE 2006

[2]. Bin Zhang, Kuizhi Mei, Member, IEEE, and Nanning Zheng, Fellow, IEEE

"Reconfigurable Processor for Binary Image Processing"in proc,IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 23, NO. 5, MAY 2013

[3]. Chih-Hsuan Tzeng, Zhi-Fang Yang, and Wen-Hsiang Tsai, Senior Member, IEEE"Adaptive Data Hiding in Palette Images by ColorOrdering and Mapping With Security Protection" in proc IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 52, NO. 5, MAY 2004.

[4]. Jayshree Ghorpade, Shamika Mukane, Devika Patil, Dhanashree Poal, Ritesh Prasad, "Novel Method for Graphical Passwords using CAPTCHA",in proc,International Journal of Soft Computing and Engineering (IJSCE)ISSN: 2231-2307, Volume-4 Issue-5, November 2014

[5]. Márcio Portes de Albuquerque, Marcelo Portes de Albuquerque, Germano T. Chacon,E. L. de Faria, Andrea Murari, and JET-EFDA Contributors, "High-Speed Image Processing Algorithms for Real-Time Detection of MARFEs on JET",in proc IEEE TRANSACTIONS ON PLASMA SCIENCE, VOL. 40, NO. 12, DECEMBER 2012