International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

CAPTCHA: A New Security Approach by Using Graphical Password

Pritesh Patil[1],Mohammad Hayat[2], Azad Mehatkar[3], Sraddha Bose[4]

[1,2,3,4] *Information Technology, AISSMS IOIT*

Abstract— One of the most important field in our modern technology is related to protecting the information and securing it. We are going to develop a new security primitive that isCaptcha as graphical passwords. A Captcha is an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart." The normal scenario for protection or security against attacks is unique user name and password, but this kind of security is normally breached and various attacks are being performed. Captcha provides security against attacks performed by bots. The introduction of Captcha as graphical password will addresses a number of security problems like online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. The generation of Captcha requires a number of algorithms and there are various types of captcha's that can be used. Using Captcha as password will avoid or make it impossible for the hacker to make brute force attack or guessing attacks. Captcha as graphical password will add new degree of protection thus making the data more secure and safe. Now-a-days the count of online banking and other transaction services users is increasing with a large number; this approach acts as a new security level to these services.

Keywords— Capthcha, Graphical Passwords, Bots, Security, Authentication.

I. INTRODUCTION

The security is fundamental and one of the most important task of a system. The hard AI (Artificial Intelligence) problems are useful to improved security because they are computationally difficult to solve. The Captcha is remarkable concept which represents a test to differentiate human users from computers. i.e. a puzzle, beyond the capability of computers but easy for humans. However, this new standard is used to differentiate bots and human users restricting its success.

We introduce a new security technique based on hard AI problems, Captcha technology based on graphical passwords, which we call CaRP (Captcha as Graphical Passwords). CaRP is click-based graphical passwords technique in which password is created by a particular sequence of clicks on an image, it is different than regular graphical passwords.It uses Captcha challenge in CaRP image for each attempt of login a new CaRP image is generated. Text Captcha and image-recognition Captcha both are used in CaRP. Similar to text passwords a text CaRP contains sequence of characters which is submitted by user by clicking in correct sequence on right characters. CaRP can successfully defend against online dictionary attacks on passwords, which have been major security threat for long time. CaRP requires users to solve a Captcha challenge at each login attempt.

II. BACKGROUND AND RELATED WORK

2.1 Graphical Passwords

There are several graphical password methods. Recognition, recall and cued recall these are the three methods of graphical password system based on the task to memorize and recognize the password involved. In recent review more methods can be found. A recognition based technique requires identifying among lures the visual objects belonging to the password portfolio.

The scheme is Passfaces in which a user creates password by choosing a set of faces from a database. In authentication, user selects a face belonging to her portfolio from a panel of faces represented to her. This method is repeated many times, each time containing a different set of faces.

In each round locations of images are permuted but set of images panel remains the same. Correct selection in each round leads to successful login. In a cued-recall scheme, an external cue is provided to user to easily memorize and enter a password.

Systems typically require users to remember and specific points present in an image. PassPoints is click-based cued-recall scheme in which a user selects particular points anywhere on an image by clicking on them thus creating a password and user must click on those points while authenticating. Cued Click Points (CCP) uses deterministic function to select next image and it uses one click per image and it is similar to PassPoints. Persuasive Cued Click Points (PCCP) extends CCP by requiring a user to select a point inside a randomly positioned viewport while generating a password, resulting in more randomly distributed click-points in a password. Among the three types that we have studied recall is the hardest for human memory while recognition is the easiest. Recognition is typically the weakest in resisting guessing attacks.

2.2 Captcha

Captcha depends on the gap of capability between humans and bots in solving certain hard AI problems. There are two types of visual Captcha: Text Captcha and Image-Recognition Captcha. The Image Recognition Captcha is based on recognition of non-character objects and text Captcha depends on character recognition. Security of text Captcha has been thoroughly studied.

The following mentioned principle has been established: The character segmentation, which is computationally expensive and combinationally hard text Captcha should use this. The machine recognition of non-character objects is more complicated than character recognition. The difficulty of object identification or classification, possibly merged with the difficulty of object segmentation is the key points of IRC. Asirra relies on binary object classification: a user is asked to find 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 which are computationally expensive and combinationally hard text Captcha should use this. IRCs based on binary object classification or identification of one concrete type of objects are likely insecure. Binary challenges are considered much easier than Multi-label classification problems. Captcha can be circumvented through relay attacks whereby Captcha challenges are relayed to human solvers, whose answers are fed back to the targeted application.

III. CaRP

CaRP is nothing but combination of Captcha and Graphical Passwords. CaRP is a techniques used to develop an image Captcha so as to provide additional security to the desired system. The normal security techniques used till now are vulnerable to many attacks like online guessing attacks, replay attacks, brute force attacks, shoulder surfing etc. The introduction of CaRP provides additional security to the applications and or systems thus avoiding the vulnerable attacks.

3.1 Captcha Authentication

CAPTCHA means Computer Automated Public Turing Test to tell Humans and robots Apart. Captcha authentication is normally used to detect bot attacks as bots are unable to type the characters or number in the Captcha. Captcha can be further classified as:

1. Click Text
2. Captcha Animal
3. Animal Grid

These are some types of Captcha and the use of Captcha makes it difficult for the spyware to detect the password thus providing more security and authentication.

IV. CaRP OVERVIEW

The Captcha is converted to the CaRP image. The CaRP image avoids the exploitation of hotspots and thus makes it difficult for the hacker or attacker to guess the clickpoints selected by the legitimate user.

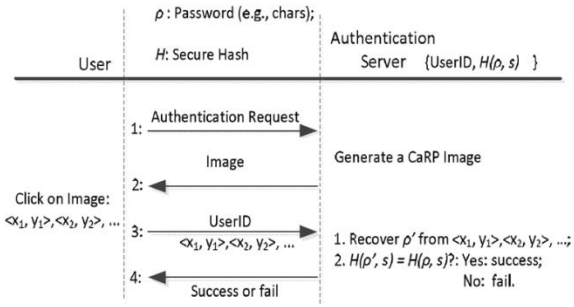

Fig.1 Working of the System

The above figure depicts the flow of proposed system. The authorized user will enter his username and password. After entering the username and password the user will be shown a CaRP image that he selected during the registration process. Now the user will click on the click points selected by him during the registration process. As soon as the user selects one clickpoint the co-ordinates of that point will be extracted by Optical Recognition process (OCR) algorithm.

The extracted co-ordinates will then be hashed using SHA-1 algorithm. These co-ordinates then will be stored and then will be verified during every login attempt of that particular user. If the values in database and the selected hashed co-ordinates values match then the user in authenticated user and he will be allowed to access the site according to his privileges.

V. IDENTIFICATION AND RECOGNITION BASED SYSTEM

The system need to identify the entered co-ordinates properly so as to detect whether the user is a legitimate user or it is an attacker or hacker trying to gain access of the user's account. This can be done with the help of Optical Character Recognition (OCR). OCR uses clickText and Persuasive clickpoint algorithm so as to extract the co-ordinates.

5.1 Click Text

Fig.2 ClickText Point Recognition

The above figure defines how the clickText works. The cross marks on the inner part of Alphabet A are called as inner points where as the points in the external points of A are called as external points. The internal points help determine the alphabet or character by comparing the pixel colour and hence even giving the co-ordinates of that point. The external point gives the external co-ordinate.

VI. Security Concepts and Issues

Cyber security is the most important issue to tackle. Various user authentication methods are used for the security purpose. It helps to avoid misuse, disruption or illegal use of highly sensitive and confidential data. Security concepts mainly rely on confidentiality, Integrity and availability.

Confidentiality describes the authorization mechanism, which grants the user or administrator the access permission to proceed for consumption of the facilities.Integrity ensures that the data being transmitted is not tampered or modified during transmission and it has been send by the authorized user.

The principle of availability states that the resources and facilities should be always available to the users as per their requirement and schedule. It makes sure that the information required by the users is available to them anytime, anywhere as soon as possible.

6.1 Hash algorithm

Hash is the mechanism which provides the authentication and protection to the data and information which is to be stored in data base or have to be transferred from a sender to receiver. In our project we are using SHA1 hashing algorithm.

6.1.1 Secure Hash Algorithm-1

SHA-1 is the most secure Hash algorithm. It is applicable for any input message that is less than 2^64 bits in length. The output of SHA is a message digest, which is 160 bit in length.
SHA is designed to be computationally infeasible to obtain the original message from the given message digest and to find the messages producing the same message digest.
The working of SHA:

6.1.1.1 Padding:

Add padding to the end of the original message in such a way that the length of the message is 64 bits less of the multiple of 512. Padding is always added, even if the message is already 64 bits less of a multiple of 512.

6.1.1.2 Append Length:

The length of the original message is calculated and append to the end of the padding as a 64 bit block. It excludes the padding length for the original message length calculation.

6.1.1.3 Divide the input into 512-bit blocks:

The input message is divided into blocks, each of the length 512 bits.

6.1.1.4 Initialize chaining variable:

In SHA algorithm we want to produce a message digest of length 160 bits, we need to have five chaining variables.

6.1.1.5 Process Block:

Copy the chaining variable A-E into a-e. The combination of a-e, called abcde, will be considered as a single register for storing the temporary intermediate or final results.Divide the current 512-bit into 16 sub-blocks, each consists of 32 bits.

SHA has four rounds, each round consisting 20 iterations.Each round takes the current 512 bit blocks, the register abcde and a constant K[t] as per three inputs. It then updates the contents of the register abcde using the SHA algorithm steps.

There are total 80 iterations. The logical operation of a single SHA iteration can be shown as:

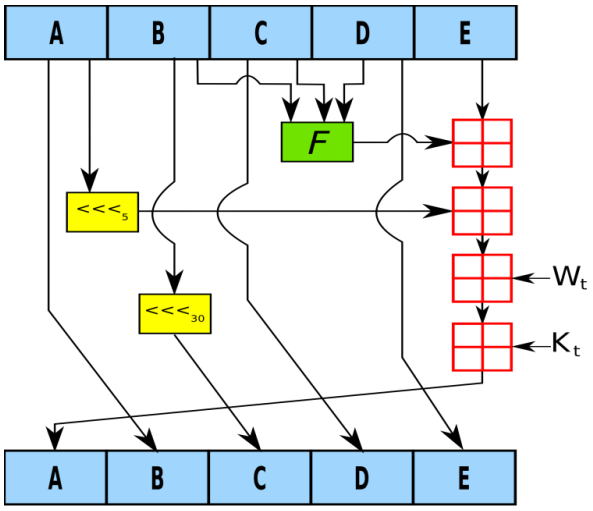

Fig.3 Working of SHA-1

6.2 Replay Attack:

It is a type of network attack in which a valid data to be transmitted is maliciously repeated or delayed. The attacker tries to intercept the data and retransmits it, possibly as a part of a masquerade attack by IP packet alteration or substitution. The authentication, conversation between the sender and receiver and information eg- exchanging of key to invoke the receiver is compromised in this type of attack.

6.3 Brute Force Attack:

Brute force attack is a cryptanalytic attack which is used against encrypted data. It is also known as exhaustive key search. It is the type of attack where the attacker or hacker tries to access the resources by unauthenticated guessing of possible passwords generated by the user.

The attacker tries to calculate every possible combination that could make up a password and then test it to see if it is the correct password. With increasing password's size, the amount of time duration, on average, to find the correct password increases exponentially. This means the passwords with short length can usually be discovered and guessed quite quickly and in short interval of time but longer passwords may take decades.

VII. CONCLUSION

It is a new security primitive relying on unsolved hard Artificial Intelligence difficulties. This approach is the combination of both a Captcha and a graphical password mechanism. The motive of this approach introduces a new version of graphical passwords, which adopts a new security approach to eliminate online guessing attacks: a new captcha image, which is also known as a Captcha challenge, is used for all login attempts to make the trials or efforts of an online guessing attack completely independent of each other. A password in this approach can be found only possibly by automatic online guessing attacks which include brute-force attacks; a desired security features that other graphical password mechanisms lack. ClickText had better password memorizing potential than the conventional text passwords. On the other hand, the usability of Captcha as a graphical password can be further rectified and strengthens by using images of various levels of difficulty based on the login history of the user and the machine used to login.

REFERENCES

1. 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. [2] (2012, Feb.). The Science BehindPassfaces [Online]. Available:http://www.realuser.com/published/ScienceBehindPassfaces.pdf
2. B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161–170
3. 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. 128–21, Jan./Feb. 2012.

4. J. Yan and A. S. El Ahmad, "A low-cost attack on a microsoft CAPTCHA," in Proc. ACM CCS, 2008, pp. 443–444.
5. H. Gao, X. Liu, S. Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in Proc. Symp. Usable Privacy Security, 2009, pp. 760–767.
6. L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using CAPTCHA in graphical password scheme," in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010, pp. 1–9.
7. K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, "Building segmentation based human-friendly human interaction proofs," in Proc. 2nd Int. Workshop Human Interaction Proofs, 2004, pp. 1–10.

