"A ROBUST AUTHENTICATION SCHEME WITH CAPTCHA USING ENHANCED SECURITY PRIMITIVE"

[1]GUNJAN MALVIYA
PG Department of Computer Science &Technology D.C.P.E H.V.P.M, Autonomous College, Amravati, India
gunjanbr82@gmail.com

[2]PALLAVI ITANKAR
PG Department of Computer Science &Technology D.C.P.E H.V.P.M, Autonomous College, Amravati, India
pallaviitankar@gmail.com

ABSTRACT: *All the applications on web implement varied authentication schemes to secure data from unauthorized access. Without proper authentication scheme the data is subjected to be attacked. Passwords are most widely used form of authentication scheme. Lot of researches has been done to make this scheme better and more secure. Still there is lot of scope as this form of authentication schemes has several vulnerabilities such as eavesdropping, replay attack etc. One more type of attack which is been a trouble for service providers is Denial of Service (DoS) attack sometimes called as botnet attack. This is an attempt to make a machine or network resource unavailable to its intended users by flooding it with useless requests/traffic. CAPTCHA is a possible solution for such DoS attack. But programs are designed to bypass the CAPTCHA security. In this work we make an attempt to present a robust authentication scheme using modified process of CAPTCHA to enhance authentication security at input level. The proposed scheme is supposed to be security measure for number of attacks such as eavesdropping, replay attack, and botnet attack.*

Keywords: Captcha, Denial of service, authentication, botnet attack.

1. INTRODUCTION

Networks, both internet and intranet provides numerous ways to connect, communicate, share and access your public or private data worldwide, but not without some risk. The first step toward securing a computer system is to have some authentication to verify the identity of users. Authentication is the process of determining if a user or identity is who they claim to be. Authentication can be accomplished using different methods and techniques. It is very important which authentication technique or method to use, which may vary according the type of application or the environment where this is going to be applied and probably it is the most critical issue in designing secure systems. The most common computer authentication method is the conventional method in which the user has to submit a user name and text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords [3]. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords [5]. On the other hand, the passwords that contain variety of characters and special symbols so as to make it unguessable are not easy to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts.

To address the problems with traditional username password authentication scheme alternative authentication methods, such as biometrics, smart card *etc.* have been used, but they stand very complex for the small and simple applications yet requires a strong authentication. Hence, we will focus on another alternative using one time password (OTP) with different perspective.

Also the most popular attack on server to overload the server is Denial of Service attack, where bots or computer programs are designed to overload the server with predicted username and password request making the server to serve number of requests within a fraction of second to which server cannot respond and server crashed because of these flooded request [6]. This is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. CAPTCHA is a possible solution for such DoS attack.

The basic purpose of a CAPTCHA (an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart") is a type of challenge-response test used in computing to determine whether or not the user is human [7]. Captcha is a new security standard technology to preserve our emails, messages and other services online social websites from the online computer programs generally called as bots. However, this new security standard for identifying bots has achieved just a limited success as the complex computer programs are designed to bypass the CAPTCHA security using image processing and alike domains.

Is it possible to create a robust authentication scheme over traditional one and to create any new security primitive based on Captcha for DoS attacks? This is a challenging and interesting open problem.

Hence, here we propose a robust authentication scheme using Captcha as Enhanced Security Primitive (RASCESP), introducing a security for the users so they can browse safely and their personals will be safe using RAS and providing security from bots to server using CESP.

2. EXISTING SYSTEM

Captcha is used for online security purpose but now a days the implementation of text based Captcha is very simple. The Captcha is basically used as a computer program or system to distinguish human from machine input during extraction of data from website. It is very useful and requires a large question bank. A primary task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable to identify the correct characters and

digits. The text based Captcha is possible to identify the character and digit through Optical character recognition (OCR) technique. Text based Captcha is a combination of characters and numbers that continuously generate the random Captcha by the system but for the human it is somewhat difficult to remember the long string of number and character as a password as compare to the graphical Captcha and also after some day's bots is program which is automatically created the number of accounts of one user which is major problem for security. So here we can say that text based Captcha provides a less security.

[1] Nowadays, numbers of graphical password schemes have been proposed and these schemes are classified in three categories based on the task involved such as recognition, recall and cued recall. In recognition based scheme, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he/she selected during the registration stage. In the recall based scheme, a user is asked to reproduce something that he/she created or selected earlier during the registration stage. In cued recall based scheme, the hint is provided for the user to memorize the password and then user can enter the password. Image-based Captcha are challenge-tests in which the users have to identify the image that is asked to user therefore, it is difficult to break this test using pattern recognition technique.

Hence, there is a need to introduce another strong security scheme which is not easily recognized by the bots.

3. IMPLEMENTATION PLAN

RAS is the improved conventional authentication scheme where user's password will be updated and notified via email every time the user login. This updating of password involves the process of (OTP) One Time Password keeping user's password as it is just appending some sort of random text or digits (OTP) with such a length those have a large number of permutations making it unable to guess. We call this scheme as dynamic password. This scheme makes the password more authentic and strong solution to Guessing Attack and Shoulder Surfing Attack.

CESP is a random group small image cascaded in single image, where the user has to identify an image as per asked question. For e.g. group of image contains 20-25 bird images and user is asked to identify a particular bird amongst group by clicking on the particular image, determining whether or not the user is human.

In our proposed model, recognition based scheme is used, presenting the random group of image to user and need to identify asked image.

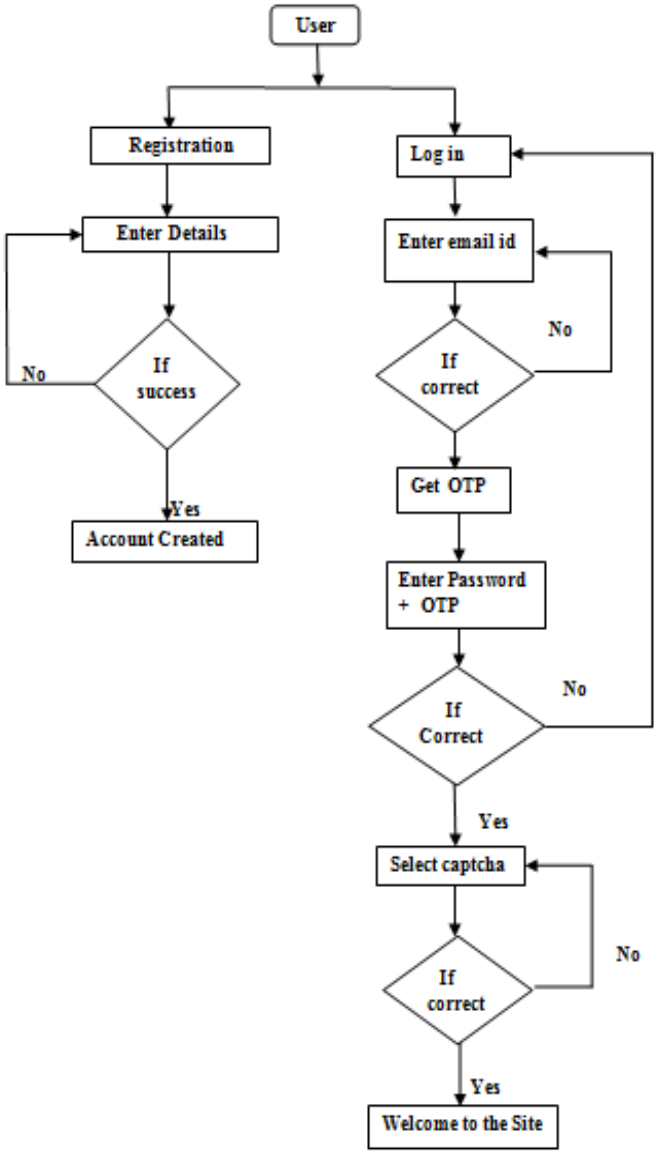

Figure 1: Proposed System DFD

4. CONCLUSIONS AND FUTURE SCOPE

Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument.

The future research should concentrate on improving the login time and memorability. When a user inputs the corresponding substrings which belong to different CAPTCHAs, the time gap is longer than the time between two characters in one substring. So a method for narrowing the time gap in the entering process and reduction of the impact of users choice trend on security, provide other areas for future research. Also, one can work on presenting each separate user with separate captcha images.

5. REFERENCES

[1] Bin B. Zhu et. al., "Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems" IEEE Transactions on Information Forensics and Security, VOL. 9, NO. 6,, pp. 891-903, JUNE 2014

[2] Mughele Ese Sophia "Three – Level Password Authentication" European Journal of Computer Science

And Information Technology Vol.3, No.5, pp.1-7, November 2015

[3] M. Kameswara Rao et. al., "A Novel Graphical Password Authentication Mechanism for Cloud Services" Information Systems Design and Intelligent Applications, Springer India, Volume 433 of the series Advances in Intelligent Systems and Computing, pp 447-453

[4] Suo, Xiaoyuan, "A Design and Analysis of Graphical Password." Thesis, Georgia State University, 2006.

[5] Xiaoyuan Suo "Graphical Passwords: A Survey", Department of Computer Science Georgia State University http://scholarworks.gsu.edu/cs_theses/27

[6] https://en.wikipedia.org/wiki/Denial-of-service_attack

[7] https://en.wikipedia.org/wiki/CAPTCHA