ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Two Way Authentication for Web Services using Video CAPTCHA and Kerberos

Pranal Tayade, Prof. Mahip Bartere

ME CSE (Scholar), Dept of Computer Science, GHRCEM, SGBAU Amravati University, Amravati, India

Asst. Professor, Dept of Computer Science, GHRCEM, SGBAU Amravati University, Amravati, India

ABSTRACT: With growing use of internet and its services, a large number of organizations are making use of password to provide security. The password is most convenient means of authentication. But now a day's password becomes hacked by the attacker. To provide more security, we are using Kerberos and the video CAPTCHA as authentication technique. Kerberos is a authentication protocol and CAPTCHA is a (Completely Automated Public Turing Test to tell Computer and Human Apart) test which provide a way to differentiate user into a human and malicious program. CAPTCHA become the most widely used standard security technique to prevent automated computer program attack. Our aim is to proposed a system which can be a better than existing CAPTCHA and provide higher level of authentication.

KEYWORDS: CAPTCHA, Kerberos, video CAPTCHA.

I. INTRODUCTION

Internet has become an indispensable part of daily transactions including shopping, education, Commerce and industrial sector. All these transactions mainly needs to enter individual information in certain registration forms and then only the user is allowed to access that website. But some individuals develop a program which makes false registration by filling wrong information and access the website. It results in the wastage of web resources. So in this way the malicious programmers or robots try to deny the services used by the regular users. There are various methods introduced to prevent these attacks. It is difficult for humans to examine the huge and bulky data of registration. Some methods are implemented with the help of computer in order to distinguish human users from computers. To distinguish between human and machine a test known as Turing test is used in which the right judgment is made by providing intelligence to computer.

First time CAPTCHA was invented in 2000 at Carnegie Mellon University by John Langford, Nicholas J. Hooper and Luis Von Ahn [1]. CAPTCHA is an acronym for "Completely Automated Public Turning Test to tell Computers and Humans Apart" [2]. Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHAs) are a class of automated challenges used to differentiate between legitimate human users and computer programs (`bots') on the internet. CAPTCHAs have many practical security applications, including preventing the abuse of online services such as free email providers. The need for a more secure yet user friendly CAPTCHA arises.

A CAPTCHA system must satisfy the following three characters:

1) Human can recognize the contents and pass it easily.
2) It is invoked to prevent robots to pass the system or to increase the processing cost through continuous attack.
3) It should be generated easily and quickly. CAPTCHAs have several applications for practical security,

CAPTCHA is an authentication process based on challenge response authentication. CAPTCHA provides a mechanism with the help of which a user's can protect them for spam and password decryption by taking a simple test. In this test a user will see either an image or a text which are normally distorted. The user is supposed to enter the pattern exactly as shown to him if the CAPTCH is based on text. If the CAPTCHA is based on image the user is supposed to enter the correct name of the image which correctly symbolizes the image. CAPTCHA is used where authenticated access is the primary concern.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

II. RELATED WORK

Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu**,** suggest a new security is emerging as an exciting new paradigm, 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. 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 offers reasonable security and usability and appears to fit well with some practical applications for improving online security**.** AnimalGrid and ClickText easier to use than PassPoints and a combination of text password and CAPTCHA. Both AnimalGrid and ClickText had better password memorability than the conventional text passwords. On the other hand, the usability of CaRP can be further improved by using images of different levels of difficulty based on the login history of the user and the machine used to log in [3].

With the growing use of Internet and its services, a large number of organizations are making use of it to provide and seek information of the people using those services. This has raised the chances of attacks on such services by interrupting them sending multiple requests to the servers providing these services programmatically. So a new technique that utilizes image from custom mouse cursors and outperforms some most popular CAPTCHA techniques such as Text – based CAPTCHAs and previous Image – based CAPTCHAs [4].

Baljit Singh Saini, Anju Bala, gives a CAPTCHA scheme that can be used to distinguish human and robot such as malicious program. Both Google and Microsoft use the text-based CAPTCHA for authenticated process. However, all text-based CAPTCHA has been broken due to the fact that it can't prevent Optical Character Recognition (OCR) attack which can automatically identify the CAPTCHA's words. Consequently, new kinds of CAPTCHA have been proposed to solve this security hole. For example, image-based and audio-based CAPTCHA are new emerging schemes used to replace text-based CAPTCHA. Here, they propose a novel CAPTCHA scheme (GeoCAPTCHA) which utilizes the personalized contents such as geographic information to prevent the 3rd Party Human Attack. Then, we conduct a security analysis of the usability and security of GeoCAPTCHA. GeoCAPTCHA can enhance the performance and security of the Google and Microsoft's CATPCHA system with rotated 3D street-view image [8].

As many text-based schema have been broken OCR techniques, a new 3D CAPTCHA have emerged. Here the study of robustness of 3D text-based CAPTCHA adopted by Ku6 which is a leading website providing videos in China and also provide the first analysis of 3D CAPTCHA. The security of this CAPTCHA scheme relies on a novel segmentation resistance mechanism, which combines Crowding Character Together (CCT) strategy and side surfaces which form the 3D visual effect of characters and lead to a promising usability even under strong overlapping between characters [1].

The prevailing implementation of CAPTHA is 2D still image verification code however; the developing AI and image recognition technology makes it possible for computer program to pass through CAPTCHA's test. So a new CAPTCHA implementation which is in the form of 3D animation based on the week point of computer vision. New method prevents attacks based on image recognition and moving object recognition [9].

Turing test to tell Computers and Humans Apart, it's become a key to prevent malicious programs to access web resources automatically. A new type CAPTCHA system will be proposed. The proposed scheme, named Clickspell, combined the features of text-based and image-based CAPTCHAs. Clickspell asks users to spell a randomly chosen word by clicking distorted letters for passing the test. Users can learn the definition(s) of the chosen word. Clickspell can add an advertisement image which in turn increases Security of your system [7].

Baljit Singh Saini et al. [2] In this paper, they examines CAPTCHAs and its working and literature review and they also describes classification of CAPTCHAs and its application areas and guidelines for generating a CAPTCHA. To implement the CAPTCHA there are three methods: Visual method, OCR (Optical Character Recognition) and non OCR visual method. In this paper they are comparison types of CAPTCHAs. This paper gives a description for various existing CAPTCHA schemes with a literature survey and provides a description for working of CAPTCHA. This is also describes the classification of various CAPTCHA schemes. And finally, the various applications of CAPTCHAs and comparison between OCR and NON-OCR based CAPTCHAs are also presented.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

III. PROPOSED ALGORITHM

A. *System Implementation*

In a propose work, we are going to propose a system which provide a multi-level security to the web services. In a propose system we were using the authentication protocol i.e Kerberos and a video CAPTCHA which provide higher authentication and security to services. Kerberos is authentication protocol which work on the basis of ticket to allow nodes communicating over a network to prove their identity to one another in a secure manner. CAPTCHA is a turning test created by computer or program for user who is expected to be a human. The test is easy for human but difficult for any machine. The user is required to provide the correct response to the test and then user permit to access the work. When correct response is received then it conform that the response arrived from human and not from program or machine.

Total work can be divided into following module:

1. Development of Kerberos

Kerberos is an authentication system that uses symmetric key cryptography to protect sensitive information on an open network. It is a ticket based system in which Kerberos server issues a ticket encrypted with the user's password when the user logs in. It consists of the three parties. Those are the client, the server and the key distribution server. Whereas the key distribution Centre consists of authentication server and ticket granting server.

2. Collection of video data set.

In this module various online data set like trecvid will be studied and used for a project. Video data set are publicly available.

3. User signup process.

In this module the user will sign up based on username, password, video, video sequences object. This will save the entire video with the sequence for the user to the database.

4. User login.

In this module Kerberos authentication with video compare, video sequences compare, video sequence object compare will be used to login the user.

5. Result evaluation and optimization

In this module result will be evaluated and system will be optimized if required. In this module we are comparing the outputs of video CAPTCHA and the existing CAPTCHA (i.e image based CAPTCHA).

B. *Description of the Proposed Algorithm:*

Aim of the proposed algorithm is to provide the security to web services for that we are using video CAPTCHA and Kerberos as standard authentication protocol. Our aim is to provide two way authentications to propose system one is with Video CAPTCHA and other is with Kerberos which uses a following algorithm.

```
    L1:  un, pwd, t1-> request submission time.
     If un and pwd is matched with database
      Goto L2;
     Else
     Goto L1;
L2: t2-> login time,
    If t2 - t1< maxtime;
    Goto L3;
    Else
    Goto L1;
L3: Ticket,
    If Ticket is matched,
    Grant Access to services
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Else
Goto L1;

In proposed algorithm there are three levels, in first level when user enters the user name and password in login process. When username and password is matched with the database then goto level two along with request submission time. In level two, t2 i.e. login time. When t2-t1 is less than the maxtime then goto next level. If t2-t1 is greater than goto level one. In level three, ticket is present to the user, in the ticket the username, user id, server id, and the time to live. If the contains of ticket is matched then ticket is used to access the services, otherwise it goto level one. Login time will be varying in each time.

C. Advanced Encryption Standard

The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The number of cycles of repetition is as, 10 cycles of repetition for 128-bit keys, 12 cycles of repetition for 192-bit keys, 14 cycles of repetition for 256-bit keys. Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key. Here in proposed system we are using 128 bit keys, which are used for encrypting the key which is generated from the user's password, and also for decrypting the key. Also we are using AES for encrypting and decrypting the ticket which is used by client for obtaining the ticket.

IV. DESIGN METHODOLOGY

This section focuses on methodology used to implement proposed system. The proposed system focuses on improved security for the web services to avoid from getting abuse. The architecture of system consists of the following sub-systems.

- Client registration with video CAPTCHA.
- Authentication ticket provided by server to client.

A. Client Registration with Video CAPTCHA

When user need to use the services then user required registering for services. In proposed system, we are using video CAPTCHA as a security mechanism which enhanced the existing security. As in existing system text based Captcha, image based Captcha, graphical Captcha. We are improving the security, in video CAPTCHA user need to enter the username, password, contact and email for signup process. In the signup process, user enters username, password and user clicked on the load video. Then video should be loaded, from loaded video frame are extracted and assign a tag and that tag is saved. At the time of login user need to enter the proper and exact tag. If the enter tag is matched then it process further towards services. If the entered tag is not matched then it goes to the login page and same process is repeated. Extracted frames may be in sequence or we can skip the frame and saved the tags. User had to set the three frames compulsorily, and if user wants to set more frames then user can set the frame.

B. Authentication Ticket Provided By Server to Client

As we are going to provide a multi level security for web services. Firstly by using the video CAPTCHA and secondly by using the Kerberos which is based on the granting ticket to used the services. The working of the Kerberos is based on the ticket. Kerberos consist of ticket granting server which provide the ticket to user to used the services and the authentication server which authenticate the details of the user and also decrypt the contain of the ticket. Kerberos consist of the key distribution centre and the application server. And then the user send this TGT encrypted with key to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

TGS to provide the ticket to used the services. Then user can decrypt using key and see the details of ticket which contains the user name, user id, server id, and time to live. Then user used this ticket and enters it if matched then user is able to use the services. Otherwise repeat the same process again.

In the first phase, the client sends a request to the Kerberos Authentication Server (AS) requesting a ticket granting ticket to be used in the second phase with the Ticket Granting Server (TGS). The AS is expected to reply with a message consisting of the ticket granting ticket and an encrypted component containing a fresh session key to be shared between the client and the TGS.

In the second phase, the client forwards the ticket granting ticket, along with an authenticator encrypted with the session key obtained in the first phase, to the TGS, requesting a service ticket to be used in the third phase with the application server. The TGS is expected to reply with a message consisting of the application server ticket and an encrypted component containing a session key to be shared between the client and the application server.

In the third phase, the client forwards the application server ticket, along with a new authenticator encrypted with the session key obtained in the second phase, the application server, requesting certain service. The application server ticket plus the secret session key are the client's credentials to be authenticated to a specific application server. If all credentials are valid, the application server will authenticate the client and provide the service.

C. Flow Chart of System

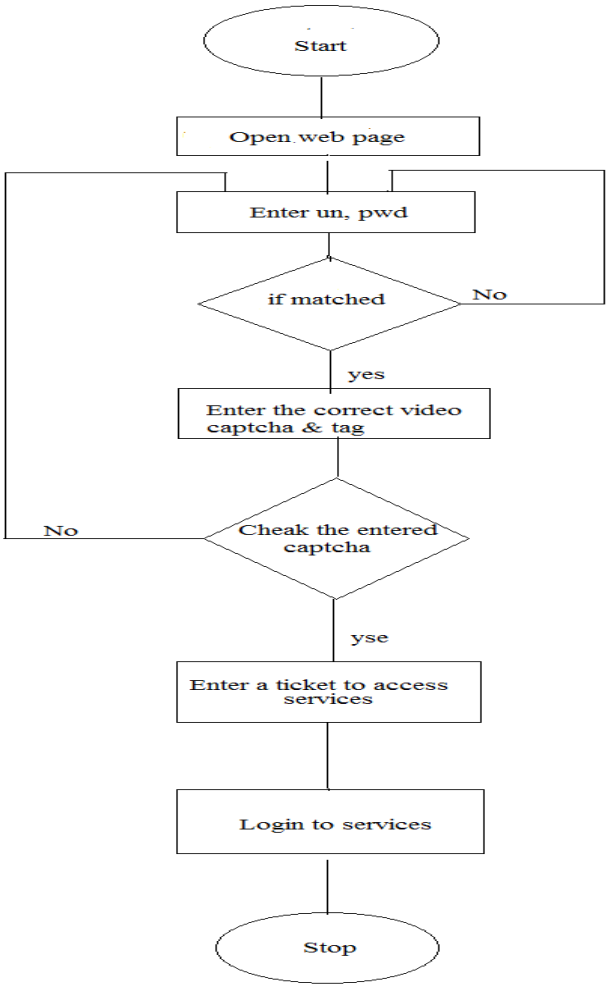

Figure: Flow chart of the system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

V. CONCLUSION AND FUTURE WORK

The Various CAPTCHA alternatives are continuously emerging, and this race will continue and more advance. The basic idea of CAPTCHA is to tell computer and machine apart and this concept is worth to be discovers for several reason. We have proposed the first CAPTCHA that uses video understanding to distinguish between humans and machines. As a contribution toward improving the web security in the field of an automated challenge and response against attacks issued by automated programs, we proposed a more robust video based CAPTCHA. Since a weak CAPTCHA implementation can only provide a false sense of security, we have been addressing the principle features which contribute in effective way to provide more secure challenge. We explore the security and usability of video CAPTCHA, and to propose a system which can be a better system than existing CAPTCHA and also provide higher level of authentication using Kerberos.

In future we can provide multiple challenges to user so that the security will improve. Also we will try to implement this in mobile with android operating system. The video Captcha have more future scope where the quality of video should be improved, and also try to minimize the memory space.

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. Nikitha Bhasu and Raju. K. Gopal, "Enhanced Security Solution to Prevent Online Password Guessing Attacks,"*SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) – volume1 issue6 August 2014.*
3. Qi Ye, Youbin Chen, Bin Zhu, "The Robustness of a New 3D CAPTHCHA," *11th IAPR International Workshop on Document Analysis Systems, 978-1-4799-3243-6/14 $31.00 © 2014 IEEE*
4. Sanket Bhat, Saumitra Damle, Priyanka Chaudhari, Abhijeet Saraogi, "KERBEROS: An Authentication Protocol," *International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 2, February 2014.*
5. Varun Ambrse Thomas, Karanvir Kaur,"Cursor CAPTCHA –Implementing CAPTCHA Using Mouse Cursor ,"*978-1-4673-5999-3/13/$31.00 ©2013 IEEE.*
6. Chundong Wang, Chaoran Feng, "Security Analysis and Implement for Kerberos Based on Dynamic Password and Diffile-Hellman Algorithm, "*Fourth International Conference on Emerging Intelligent Data and Web Technology, 2013 IEEE.*
7. Nipun Manohar, Yogesh Kusmude, Chetan Konde," A Spelling Based CAPTCHA System Using Click, *"International Journal of Computer Science and Management Research, Vol 2 Issue 4 April 2013.*
8. Te-En Wei, Albert B. Jeng," GeoCAPTCHA - A Novel Personalized CAPTCHA Using Geographic Concept to Defend Against 3rd Party Human Attack,"*978-1-4673-4883-6/12/$31.00 ©2012 IEEE.*
9. Jing-Song Cui, Jing-Ting Mei, Wu-Zhou Zhang, Xia Wang, Da Zhang," A CAPTCHA Implementation Based on Moving Objects Recognition Problem," *International Conference on E-Business and E-Government, 978-0-7695-3997-3/10 $26.00 © 2010 IEEE.*
10. Catargiu Raluca, Borda Monica, "USING KERBEROS TO SECURE TLS PROTOCOL,"*978-1-4244-8460-7/10/$26.00 ©2010 IEEE.*
11. Eman El-Emam, Magdy Koutb, Hamdy Kelash, and Osama Farag Allah," An Optimized Kerberos Authentication Protocol*," 978-1-4244-5844-8/09/$26.00 ©2009 IEEE.*

BIOGRAPHY

Miss. Pranal C. Tayade is a Research Assistant in the Computer Science Department, G. R. Raisoni, College of Engineering and Management, Amravati University. She received Bachelor of Engineering degree in 2012 from SRPCE, Nagpure, MS, India. Her research interests are Security, Network Security, etc