IJCTA, 10(8), 2017, pp. 553-557
© International Science Press

ISSN: 0974-5572

Enhance Security in photo sharing sites using Video CAPTCHA

Harshada Mhaske[1], Pratik Kadam[2], Amit Ghatge[3], Makarand Jadhav[4] and Shantanu Doke[5]

ABSTRACT

As the Internet is a boon to mankind , its services and usage has increased a lot, many organizations feel vital to use password to enhance security to their data. Password as authentication is common and widely used technique but passwords are no longer safe. So we propose using Kerberos along with video CAPTCHA. Kerberos is a authentication protocol. CAPTCHA (Completely Automated Public Turing Test to tell Computer and Humans Apart) serves as a platform to differentiate human user from bots and malicious program. Nowadays CAPTCHA is widely used and it serves as a standard security technique to prevent bot attacks. Our aim is to propose a system which could enhance the existing systems.

Keywords: CAPTCHA , Video, Server,Video CAPTCHA, KEBEROS

1. INTRODUCTION

Computer security is vital in nearly any technology- driven business that operates on computer systems. The most aim in security is to provide a scientific discipline system that square measure computationally unfeasible for attackers to achieve access to the system. Once coming up with a laptop system, there square measure several aspects to be taken into consideration, among that one amongst the most issue is security, that sway be important. For example the matter of whole number factoring could be a technique utilized in RSA.. These primitives square measure supported arduous AI problems.

CAPTCHA is a new model for standard Internet Security. CAPTCHA, also called as reverse Turing Test is a type of challenge response test which is very handy to differentiate whether the user is a human or a bot. CAPTCHA serves in protecting from spam messages and various online attacks by providing a simple test that proves whether user is a human and not a computer bot trying to gain unauthorized access or break into a password protected account.[1]

CAPTCHA can be classified into Text based CAPTCHA, Image based CAPTCHA ,audio based CAPTCHA ,video based CAPTCHA. Image based CAPTCHA has some disadvantages which is removed by using the audio based CAPTCHA and video based CAPTCHA

2. BACKGROUND AND RELATED

2.1. Graphical Passwords

Graphical Passwords consists of pictures, objects to authenticate the legal users. There are various graphical password schemes proposed. They are grouped further into Recognition based scheme, Recall based scheme and Cued recall scheme.[6][10]

[1-5] Assistant Professor, PCCOE, Akurdi, *Emails: harshadamhaske@gmail.com, kadampratik518@gmail.com, amitghatge37@gmail.com, makarandjadhav9@gmail.com, shantanusdoke@gmail.com*

2.1.1. Recognition Based Scheme:[2][3]

This scheme need identifying images related to a user's password portfolio. While creating passwords, it demands users to memorize a series of images and then identify their images to authenticate. The vital application of such system is in Pass faces where the user select images through database server to create a password. During the authentication process, a set of face's related to the user portfolio are shown for the selection. Such procedure is repeated for several rounds. A login is successful when a user select images in correct order for each round.

2.1.2. Recall Based Scheme

This scheme need user to recall and reproduce a secret drawing. It is defined as draw-metric systems. The real time application include Draw A Secret (DAS) which allows user to draw the password on a 2D grid. Then by using 2D grid system, it encodes a sequence of grid cell used for drawing password. Pass-Go enhances the (DAS) scheme by encoding only grid intersection points and not by grid cells. This scheme facilitates a foundation for strong passwords by adding background images to DAS.[4]

2.1.3. Cued Recall Scheme

It provides an external cue to help memorizing and entering the password. It is also known as loci metric system, it is also referred as click-based graphical password scheme. One vital application is Pass Points. It allows user to select some points on an image and these points need to be clicked while authentication. Cued Click Points (CCP) uses one image per click and further image is selected by a deterministic function. To enhance CCP, another scheme named Persuasive Cued Click Points (PCCP) was introduced. In these Scheme user selects a point inside a view port for creation of a password. This helps to create more complex click points in a password.[7]

2.2. Captcha as Graphical Password

CaRP technique focuses on new image for ever login process for the same user. It can thwart guessing attacks. A CaRP image includes alphabets, images, numbers etc, which leads to formation of visual objects. CaRP scheme normally is a click based graphical passwords. It is quite handy in Internet applications such as m-commerce, Internet banking, online shopping etc which uses CAPTCHA for the authentication. CaRP is further used in e-mail services so that it reduce spam emails. A user interaction is a must to authenticate into the account, so even if the bot knows the login credentials, he is restricted from accessing the e- mail services which leads to reduced spam emails.

2.2.1. Basic CaRP Authentication

Like all CAPTCHA schemes, CaRP provide user authentication phase for granting login access permissions. The authentication task is done by the authentication server. The working is done by a authentication server which save the salt value 's' and the hash value 'H' computed by H(p,s) for each and every user account while this system does not store the password p. Whenever a user's request reach to the server, authentication server generate a CaRP image and it record's the positions of the object's and send it to the user for clicking the password. A CaRP password includes some click-able points on the image or visual objects. The user clicked point co-ordinates are recorded on user side and are sent to the authentication server along with the corresponding user ID. Then authentication server maps the co-ordinates received onto the corresponding CaRP image and then it recovers the click-able points of the objects p' . Authentication server then retrieve the salt value for the givens account and compute the new hash value H(p',s). The stored hash value of user specific account and the new hash value is compared. If both the hash values are matched, then authentication succeeds. This is the working of Basic CaRP Authentication.[5][9]

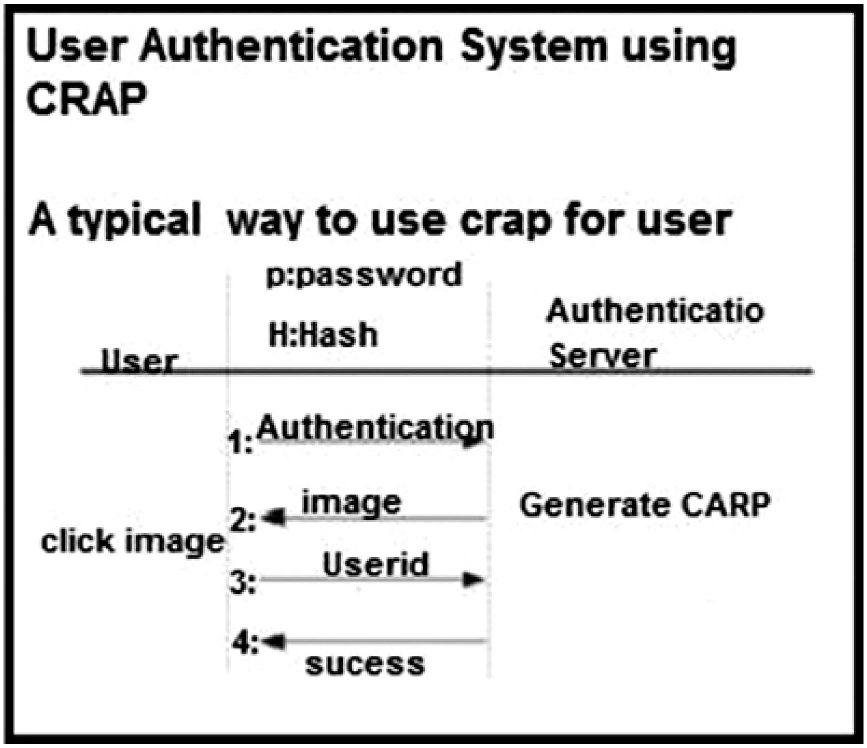

Figure 1: Data Flow diagram of proposed system

3. PROPOSED WORK

Step 1: At the time of registration user will get an video from database and provide CAPTCHA from the video as a password.

Step 2: Video clustering will take place.

Step 3: Split video into images.

Step 4: Grab unique images.

Step 5: Retrieve the text from images.

Step 6: At the time of login user will get a video to insert password(text) from that video.

Step 7: Server reproduces the text of selected password.

Step 8: If password produced is matches then go to

Step 9: otherwise it will go to step6.

Step 10: After matching of password user will allow surfing on account.

The proposed system consist of steps given below:

1) In first step the server will select the video from database and shown to the user as a password.
2) Then video clustering takes place.
3) Then this selected video is split into images.
4) After conversion of video into images we grab only unique images.
5) Then server will process this images and retrieve the text from images.
6) When user want to login user insert the text display in the video.

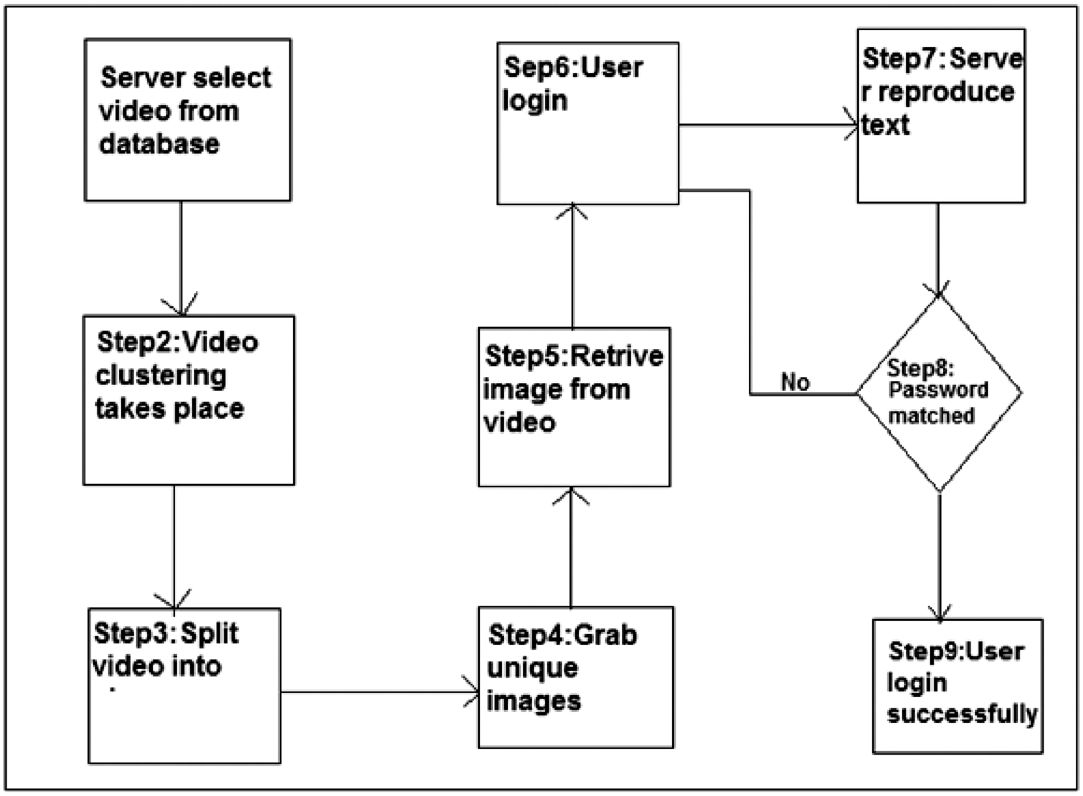
Server select video from database
Step2:Video clustering takes place
Step3:Split video into
Step4:Grab unique images
Step5:Retrive image from video
Sep6:User login
Step7:Server reproduce text
Step8: Password matched
No
Step9:User login successfully

Figure 2: Working of proposed system

7) Server reproduce the text in the video.
8) If the text reproduce by password and user text match then user has successfully login.

4. APPLICATIONS

CAPTCHA is used in various application such as

1) Email spam: CAPTCHA is used to detect spam mails.
2) E-Ticketing: By using bots some user book multiple ticket online quickly. This will detect by using video based CAPTCHA.
3) High security: By using video CAPTCHA we will provide high security to online site access such as bank account access, photo sharing sites,cloud access.
4) Computer bot program: By using CAPTCHA we prevent bot program which is used for stealing information of user.

CONCLUSION

This paper give information of different types of CAPTCHA and different types of graphical password. CAPTCHA are classified into several types i.e Text CAPTCHA, Image CAPTCHA, Audio CAPTCHA and Video CAPTCHA. We proposed new security system for photo sharing sites which will prevent online attacks such as dictionary attack. At the end we have studied various types of application such as email spam, bot program, security.

REFERENCES

[1] L. V. Ahn, M. Blum, J. Langford, “Telling humans and computers apart”.

[2] K. Chellapilla, K. Larson, P. Simard , M.Czerwinski, “Computers beat humans at single character recognition in reading based human interaction proofs”, Proceedings of the third conference on e-mail and anti-spam , 2005.

[3] P. Jayanthi and R. Divya,”CAPTCHA as graphical password-pixel based pattern recognition system,”

[4] B. Malek, M. Orozco, and A. El Saddik, “Novel shoulder- surfing resistant haptic-based graphical password,” in Proc. EuroHaptics, vol. 6, 2006.

[5] P. Dunphy and J. Yan, “Do background images improve draw a secret graphical passwords?,” in Proceedings of the 14th ACM conference on Computer and communications security, pp. 36–47, ACM, 2007.

[6] H. Tao and C. Adams, “Pass-go: A proposal to improve the usability of graphical passwords.,” IJ Network Security, vol. 7, no. 2, pp. 273–292, 2008.

[7] P. C. van Oorschot and T. Wan, “Twostep: An authentication method combining text and graphical passwords,” in E-Technologies: Innovation in an Open World, pp. 233–239, Springer, 2009.

[8] Basso, F. Bergadano. “Anti-Bot Strategies Based on Human Interactive Proofs” in handbook of information and communication Security , pp.273-291,2010. Springer

[9] A.A. Chandavale, A.M. Sapkal, “Algorithm for secured online authentication using CAPTCHA”, IEEEXpiore Published by IEEE Computer Society., 2010.

[10] R. Biddle, S. Chiasson, and P. C. Van Oorschot, “Graphical passwords:Learning from the first twelve years,” ACM Computing Surveys (CSUR), vol. 44, no. 4, p. 19, 2012.