International Journal For Technological Research In Engineering
Volume 2, Issue 10, June-2015 *ISSN (Online): 2347 - 4718*

SECURE AUTHENTICATION USING CAPTCHA IN AI SYSTEMS

Deepthi N[1], G Raghavendra Rao[2]
[1]Student, M. Tech in Computer Networks Engineering
[2]Professor and Head of Computer Science and Engineering
National Institute of Technology, Mysuru, India

Abstract: Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information etc from unsuspecting victims for identity theft, financial gain and other fraudulent activities. A new approach named as "Secure Authentication using captcha in AI Systems" is proposed to solve the problem of phishing. Here an image based authentication using Visual Cryptography (vc) is used. Visual cryptography is used to preserve the privacy of image captcha by splitting the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed only when both are simultaneously available, the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password.
Keywords: Captcha; Phishing; Captcha based password protocol (CBPA); Authentication; AI systems

I. INTRODUCTION

Online transactions are widely used today and we can notice several attacks are found. Among those attacks, Phishing is the major security threat to be prevented. Phishing is a problem for E-commerce and online banking users that aims to get online banking passwords and credit card information which are confidential for users. It is considered as criminal activity using Social Engineering techniques. Another definition is Sending an email to a user falsely to obtain Social Security and Driver's License numbers for own gain. Thus in online transactions, security should be very high and should not be easily traced. Hence a high level of security is needed in aplication. Here we introduce a new method which can be safe against Phishing named as "Secure Authentication using Captcha in AI Systems". This approach make the both sides of the system secured as well as authenticated one by verifying the user for its own identity. Mainly, the concept of image processing and visual cryptography are used. Image processing is a process of taking image as input to produce the improved form of the same image or characteristics of input image.In Visual Cryptography an image is decomposed into shares and combine the appropriate number of shares to reveal the original image.

II. EXISTING SYSTEM AND LIMITATIONS

Security Technique which is used to prevent online email & other services from being abused by bots. Phishing are forged attempts created by malicious people to pretend as real one. Like this it can steal the important information from the owners it includes techniques like tricking customer through by sending fake mails to gain sensitive information. Many techniques are used to achieve success by avoiding phishing the existing paradigm has not achieved a complete success compared with other application. Blacklist based technique has false alarm probability , it cannot defect the unauthorised access which are not in the blacklist database. Heuristic based anti phishing technique a high has a high probability to detect false & alarm failured but it is easy for hackers to used the heuristic characteristics. Assessment based technique consumes much time in processing long time is required to do calculation. So it is not best suited to prevent unauthorized access.

III. SCOPE AND OBJECTIVE

Many security related techniques based on hard AI problem are presented to solve the mimic done by the phishing. Here ,new way of security is given to the application by using captcha as graphical password (CaRP). CaRP can identity many security threats like online guessing attacks, relay attacks shoulder -surfing attacks so on the main focus is to provided high level of security to the user by accepting captcha as part of the input. Since Captcha is a better tool which fits well with some application to increase the speed of online security.

IV. PROPOSED METHODOLOGY

In the proposed system, the main idea is to concentrate on high security using Captcha for secure authentication this can be achieved using the concept of image Processing & Visual Cryptography. Graphical password system is built on top of captha technology which is called as captcha as graphical password (CaRP). Once he Captcha is generated it is sent to email id of the user who has created the account during Registration process. The key string (Password) combination of alphabets & numbers to improve security and image is asked from the user, these both are concatenated with randomly generated. The Captcha is splitted into two shares, where one of the share is kept with user & rest is stored in the server During the first login of the user, the user's share & original Captcha sent to the user both are verified for the successful logion . In this way proposed methodology has a weight towards security by authenticating the user on the both the sides of communication.

V. METHODOLOGIES GRAPHICAL PASSWORDS

The user should create account in the system before they are trying to access or searching the details present in the system, if this is not done , they should be registered first.

Like this, users are having authentication and security for sensitive information which are present in the system.

A. CAPTCHA IN AUTHENTICATION

Captcha based password protocol (CBPA) is used to counter online dictionary attacks to achieve this , both Captcha and password are used in a user authentication protocol , valid pair of username and password is required by CBPA protocol for successful login . Capatacha challenge shows denied access for an invalid pair of user name and password.

B. OVERCOMING THWART GUESSING ATTACKS

In a guessing attack, attacker attempts to guess a password for many trial to access the sensitive information stored in the system , increases in the number of guess may lead to find the correct password. So to counter guessing attacks, traditional method helps to make the password difficult to guess even after many trials using Captcha as graphical password graphical password scheme has limited success because the password can be found by brute force attack. In this approach, two types of guessing attacks are distinguished mainly automatic guessing attacks issues automatic trial and error process every time S is constructed mannually, human guessing attacks apply trial and error process.

C. SECURITY OF UNDERLYING CAPTCHA

Captcha is a secure method in this technique, which helps to login the users who have an account. Hence high level of security is ensured for any sensitive information stored in the system. Phishing activity is easily recognised if they don't have a valid username and password. Authenticated users can access the sensitive information.

VI. LITERATURE SURVEY

To analyze the background of the current project which is helpful to find out defects in the existing system and to work out on unsolved problems the literature survey should be carried out. The below mentioned topics not only illustrate the back ground of the project but also solve the problems and flaws.

A. SURVEY PAPERS

Automated challenge Response Methods [1] is an authentication mechanism which includes challenge generation module from server to interact with challenge response to interact with challenge response in client & requests for user to respond. Challenge response module calls the get response applications , this applications is installed in client machine. This response is validated by server to continue transaction. This method ensures two way authentication & simplicity this approach prevents the man in the middle attacks because response is called by browser where man interruption is not done. DNS based anti phishing approach[2] technique which includes blacklist heuristic detection. It is not usually used by the browser. Browsers like Internet Explorer 7, Netscape Browser 8.1 are important because it uses blacklists to protect users when they are accessing phishing sites. All URL present in the blacklist are verified by the administrator thus there is very low detection of false alarm detection. it contains many disadvantages like small proportion of phishing sites are identified. Three factor authentication scheme [3] called phish-secure intended to deal with counter attack phishing First factor of authorization is done by capturing the image of particular page the user wants to visit with a specific resolution & its is checked for phishing capture image is called visual image suppose an attacker creates a phishing site which will be the duplicate copy of original page to misguide the user. The approach use the visual image of visited page & calculates the mean RGB value of the image it is named as V_RGB phish secure database consists all details of authenticated pages , where its actual mean RGB many page are collected in the database named as A_RGB. This helps to find the similarity between visited pages and the pages in the database. New anti phishing method with two types of password in open ID system [4] developed for two types of passwords for anti phishing which is safe for the open ID users open ID account has two types of password are fixed & temporary password fixed password is binded to several know PC. User can login to any Know PC . User can login to any know PC by entering the temporary password , but the temporary password are obtained by accessing the mailbox or phone temporary password can be used for limited time. This method can avoid phishing effectively.

VII. SYSTEM DESIGN

The process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements is called System Design. Systems design could be observed as how the theory of application systems are designed to develop is as a product to the outside world.

A. SYSTEM ARCHITECTURE

System Architecture is the conception design in which the structure and behavior of a system can be defined. The formal description of a system is an architecture description. It is organized such a way that supports structural properties. It also defines the building blocks and also provide plan form which procurement of products can be done.

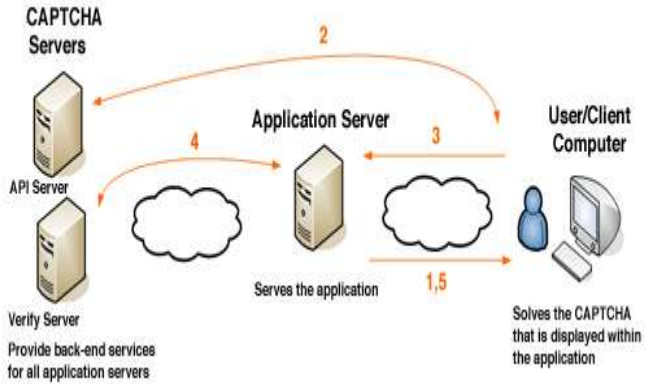

Fig -Complete architecture of Application Process

The User/Client request for registration by giving image as input, half of the image is shared in server and other half is sent to client as captcha. During first login user should enter captcha.

VIII. CONCLUSION

Phishing attacks are major problem because it capture & store the users confidential information. this information is indirectly used by phishing process then there is lack of security , data is not secured. Here phising activity is easily prevented using our proposed technique "secure authentication using Captcha in AI system "the proposed methodology secures sensitive information of users using 3 layers of security. First Layer check the user is genuine by verifying the username and password if user is not genuine they fail to entire the correct password because it is a fake one. Password image Captcha that is generated by splitting of two shares, first half with the user and the other in actual database of the server. Second layer, validates image Captcha corresponding to the user. The Captcha is readable by only human users and not by machine user. In this way we can ensure the user is permitted me or not using this image Captcha technique, machine based users cannot crack the password or confidential inform of users. Third Layer of security is intruders attacks on the user account is prevented. Users who don't have account are not allowed to use the system , this provides additional security by not letting the intruder login into the account even though they knows the username of a particular user because they fails to discover the password. Like this the proposal methodology is exteremly useful to prevent the attacks explored by phishing process.

IX. FUTURE WORK

In this approach, the image captcha is divided into 2 shares, one of the share with user & other stored in database server for future use. Finally legitimate user are allowed to access inform. This gives higher level of security due to secure authentication using capatcha. If the Captcha is stolen by intruder there is no mean of security. For that purpose ,certain pixels of image are picked randomly to calculate the mean in these situation intruder may fail to discover the password even for many trial error process.

REFERENCES

[1] J. Yan and A.S.E. Ahmad, "Three factor authentication scheme called phish-secure intended to deal with counter attack phishing," Proc. ACM Computer and Comm. Security (CCS '08), pp. 543-554, Oct. 2008.

[2] J. Yan and A.S.E. Ahmad, "New anti phishing method with two types of password in open ID system," Proc. Symp. Usable Privacy and Security (SOUPS '08), pp. 44-52, July 2008.

[3] L. von Ahn, M. Blum, N. Hopper, and J. Langford, "CAPTCHA: Using Hard AI Problems for Security," Proc. Eurocrypt, pp. 294-311, May 2003.

[4] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Automated challenge Response Methods," Proc. 17th ACM Conf. Computer and Comm. Security, pp. 162-175, 2010.

[5] Y. Xie, F. Yu, K. Achan, E. Gillum, M. Goldszmidt, and T. Wobber, "DNS based anti phishing approach," SIGCOMM Computer Comm. Rev., vol. 37, no. 4, pp. 301-312, 2007.

