Avoiding Cross Site Request Forgery (CSRF) Attack Using TwoFish Security Approach

Wasim Akram Shaik[1], Rajesh Pasupuleti[2]

[1]M.Tech in Vasireddy Venkatadri Institute of Technology, Nambur, Guntur (Dt), Andhra Pradesh, India

[2] Professor in Vasireddy Venkatadri Institute of Technology, Nambur, Guntur (Dt), Andhra Pradesh, India

Abstract: *Security is the most important factor for online users to secure their confidential data. Users are nervous about the security risks of the internet. Identifying Vulnerability has been major challenge to each user in order to rectify it. This paper addresses such type of vulnerability named as Cross Site Request Forgery attack. Basically, an attacker will use CSRF attack to trick a victim into accessing a phishing website or clicking a url link that contains malicious program which performs unwanted action that causes loss of user data. This type of attack is very effectual and dangerous to prevent it. An earlier methodology such as visual cryptography is used to avoid these CSRF attacks. Unfortunately this approach is time-consuming, as they require manual effort to integrate defense techniques which makes low accuracy rate and it not fulfill the need of the users. CSRF attacks are possible because websites are authenticated by the web browser, not the user. A novel approach "Avoiding CSRF attack using TwoFish security" is proposed to avoid these attacks by which the user can validate the website in an understandable manner. This TwoFish security is an enhanced way to validate the web page and performs authentication in two phases; Firstly MD5 encryption is performed in order to calculate the hash values for url and secondly image based authentication is provided to validate the image of respective url. By using this strategy, the user can easily recognize whether a website is a genuine website or vulnerable website. We are providing experimental results that demonstrate the use of our prototype that provides service oriented authenticated websites to respective clients.*

Keywords*: Security, Vulnerability, CSRF attack, MD5 algorithm, TwoFish, Phishing*.

I. INTRODUCTION

Internet plays a vital role in everyone's life by which we can perform most of the transactions in a less period of time. It is our basic need to perform various tasks in order to fulfill the requirements of the users in a behavioral manner. As the dependency of users on web increases, an attacker to perform vulnerability on the data may also increases. The attacks based on these webs must cause significant harm to the users. So protection must be provided in order avoid the online identity thefts [1]. The most common and popular web based vulnerability is Cross site Request Forgery (CSRF) attack [2] or sleeping giant attack [3]. It is a malicious program that modifies the user's confidential data without knowing the action ever took place. Likewise an attacker enters into victim genuine browser and can change the functionality of web application totally under his control. CSRF attack is also known as one-click attack, session riding attack and confused deputy attack [4]. CSRF attack is that exploits the trust that a site has in a user's browser. This attack targets different web applications like social media, in browser email clients, online banking, and web interfaces for network devices. Based on the web application the attacker should use the tricks like sending mails, creating phishing websites, posting messages, even changing the victim login details as username and password.

A. *Explanation of CSRF Attack with Example*

Cross Site Request Forgery attack is a common web application weakness [5], that occurs when a malicious website causes a user browser to perform an unwanted action on a trusted site on which the user is currently authenticated [6].This type of attack causes a lot of damage to the user in terms of confidential information like login details, stealing permissions, transfer of funds etc. For instance let's consider an example of customerbank.com; it is a website for online banking that allows the user for transactions, which is vulnerable to CSRF. If we visit onto the webpage and generate a request for transaction, CSRF simply accesses the user credentials and it may leads to thrashing of money. At this time an unwanted action is performed without having any involvement of the user. Let us see how the CSRF attack described above would work in a bit more detail. Assume that user logged into customerbank.com that allows for standard online banking features which includes transferring of funds from one account to other, purchasing an item. The aim of this site is trying to attack people who login into customerbank.com and setup CSRF vulnerability [7] on their site. The attacker wrote some malicious code on some intent which will perform unauthorized transaction will transfer $2500.00 to their account where the account. No is 012345678.This transfer of account should done by the attacker but the victim thinks that it is a valid operation which makes loss of amount. CSRF attack is listed among the top ten web application based vulnerabilities of 2015[8,9], It may affect the user's confidential information.

II. LITERATURE WORK

Many of the attackers creating the forged web page which contains the malicious data in order to trap the users by impersonate these web pages as real web sites. Site can be analyzed in a matter of seconds but

validation of a particular web page must be done in a proper manner otherwise it leads to loss of data to the users. Generally the creation of fake website growing in internet by which the attacker must focuses on victim to steal their confidential information. Thus creation of fake or phishing websites [10] by trapping the people is treated as phishing. These phishing web pages [11] are exactly similar to look like real ones. Victims of these attacks may rendering their confidential details like bank account details, changing passwords, accessing credit card details or some important data must be accessed by the attacker. Different techniques used by the attacker in order to tricking the customers such by sending emails, enabling key loggers and screen captures. Sending phishing Emails [12] are the most important technique to enable the phishing attack due to its simplicity and easy to use it. These emails may include malicious code which results users may lose their confidential data. Cross site request forgery is an attack, where attacker utilizes the trust that the website has on user's credentials. Currently phishing attacks [13] are so common because it can attack globally and capture and store the user's confidential information. This information is capably utilized by the attackers who are indirectly involved in the phishing process and steal the user's confidential data. Typically, phishing emails [14, 15] are trying to scam users into revealing personal information such as bank account details and PIN numbers. Researchers may propose different types of user based methodologies to authenticate the server system by avoiding phishing attacks. None of this technique may completely define this phishing attacks. A DNS based anti-phishing technique [16] like Blacklist approach is one of the popular methodology used by most of the web browser for identifying and avoiding these phishing attacks. Many organizations like Google, anti-phishing work group has provided an open blacklist query interface to the users to make an awareness regarding phishing attacks. Internet Explorer7 is one of the widely used web browser which uses blacklists to protect users when they are navigating through phishing sites. Because each url of the website in the blacklist has been clearly verified by the administrator and return the same to the user for communication, But the false alarm probability of identifying a phishing website is very low i.e. recognizing the fake websites should be fewer. It having many technical troubles like the life cycle of phishing websites is only for a few days so that a website must be shut down before we identified whether the website is a genuine website or vulnerable website.

Anti-Phishing Image Captcha validation scheme using visual cryptography [17] is used to avoid phishing attacks. The existed methodology preserves confidential information of users using 3 layers of security. A three factor authentication scheme named Phish-Secure focuses to counter attack phishing. Here as a first factor of authentication verifies whether the website is a genuine/secure or a phishing website. Second layer cross validates image captcha corresponding to the user. The image Captcha [18] is readable by human users alone and not by machine users. Here image captcha can be used to validate the user by using similarity based assessment technique [19, 20] which is encrypted and it provides authenticated process more encrypted. So using image captcha technique no machine based user can crack the password or other confidential information of users. As third layer of security it prevents the intruders attack on users account. So the earlier methods having problems while avoiding CSRF attacks like: A three factor authentication [21] is used to avoid phishing attacks require more computation time i.e. it takes too long time to calculate a pair of web pages, Here an image captcha is displayed to the user to check whether displayed image captcha must matches with the captcha created at the time of registration must provide low accuracy rate for image similarity identification. Based on the experimental results, we can specify that the existed techniques are not provide better performance in validate a webpage and fails in providing service oriented authenticated websites to the respective clients.

III. PROPOSED METHODOLOGY

In this paper a new methodology "Avoiding Cross Site Request Forgery Attack using TwoFish security approach" is proposed that provides the solution for CSRF attacks. This TwoFish security provides better way to validate the website based on the user requirement and it performs authentication in two phases; Firstly MD5 encryption is performed in order to calculate the hash values for url and secondly image based authentication is provided to validate the image of respective url web page. By using this strategy, the user can easily recognize whether a website is a genuine website or vulnerable website. To check for genuinity the user must registered into the site. After login into the site the user must submit the url and respective image of the particular webpage

for validation. This TwoFish security approach must validates webpage url, image and generate the status report regarding the webpage to specify whether it is a genuine website or vulnerable website. This is one of the best approaches to define against CSRF attack by which user can easily authenticate the website with less computation and the performance of this TwoFish methodology for calculating a pair of web pages is also efficient.

A. URL and Image Based Authentication

In this phase the user must validate the website by submitting the url and image of a respective webpage. If the url and image matches, then a message should be displayed to the user to specify that the website is authenticated website. At the same

time if there any mismatch occur then specify that the website is not genuine by specifying message as website is vulnerable website. Message Digest (MD5) is one of the standard encryption methods, which is used to encrypt the data in a very understandable manner. It takes 128 bit data as input to process the computation. Compute hash is a method which is used to calculate the hash values of the url. In cryptography, Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 128 bits. It was one of the best standard encryption algorithms. The TwoFish

Distinguishing features are the use of pre-computed key dependent s-boxes. This algorithm may provide encryption to the image which is stored in bytes. By performing encryption to the image, more safety is provided to validate the website. This TwoFish security provides two way authentications, which allows the user to validate the website in an efficient way. Whenever the user enters the url and image of a respective webpage, TwoFish approach compute the hash values of the url and at the same time compare the image of the webpage url. If the user entered details like url and image of a respective website matches then TwoFish approach returns a status message as "Authenticated website", if there is any mismatches occurs then it returns a status message as "Vulnerable website". Based on the report generated by this TwoFish approach, the user can easily authenticates the website and identifies that a particular website is a genuine or phishing website. This proposed methodology should depicts how user will authenticates the website in a well defined order by which it avoid the phishing attacks and provides service oriented authenticated websites to respective clients.

B. Algorithm Overview

The TwoFish approach is an enhanced way to avoid CSRF attack and provides authentication in two phases which is explained below:

- Firstly MD5 algorithm is used to calculate the hash values of a particular Web page url submitted by the user and store these data in a byte format.
  1) ***Compute Hash ():*** is a method in cryptography service provider to calculate the hash values of the web page url efficiently and stored the result in bytes format.
- In the second phase the TwoFish security must read the image of a web page from the user and validate it by using below functions:
  1) ***ImageConverter ():*** It is a method to convert the image into desired byte form which is used to compare the image of respective webpage url and validate it.
  2) ***EncryptStringToBytes* ():** This method performs encryption and converts string data of image into bytes.
- Finally this TwoFish approach generates a status report to the user to indicate whether a particular website is a genuine or vulnerable website.

The entire process of TwoFish Security approach can be easily understood by using Architecture method shown in Fig.1. This TwoFish security approach allows the user to validate the website and get decision regarding whether a particular website is authenticated or vulnerable.MD5 algorithm is used to calculate the hash values of webpage url and image of respective url must be read for validation and generate a report to the user to indicate which websites are service oriented authentication website and doesn't make any loss of confidential data to the users.

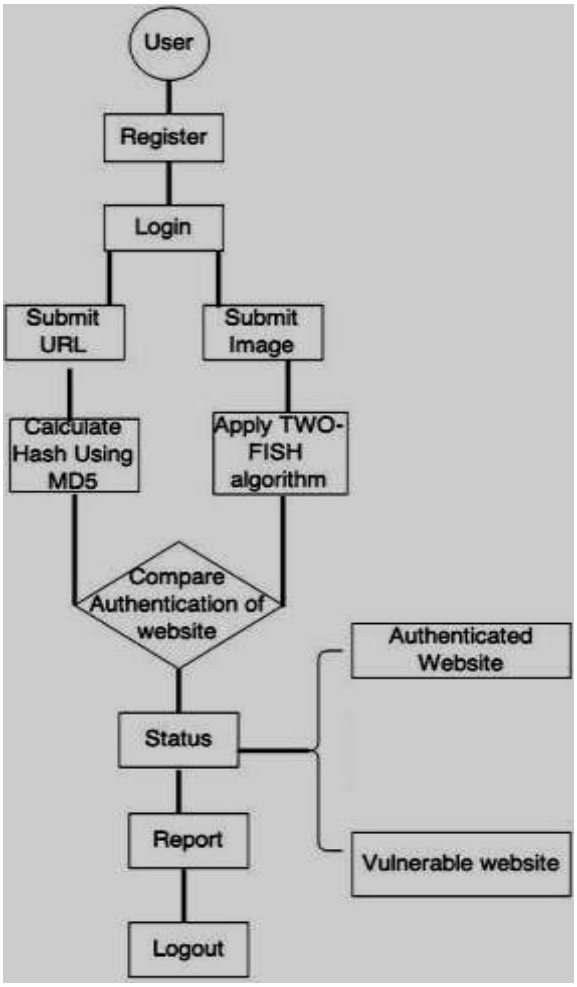

Fig.1 Architecture Diagram of Proposed Method

IV. EXPERIMENTAL RESULTS

To test our implementation, initially we gathered different websites url's and image of respective sites. All these information must be stored in a local database. Whenever user submits the url and image, the Twofish approach must validates the url and

display the status to user to indicate that a website is genuine website or vulnerable website. The submitted url and image must matched then it displays the status as Authenticated website, otherwise if the url and image selected is not matches then it specifies as vulnerable website.

The below Table 1 specify the status report regarding the url's of different websites and generate a decision to know whether a particular website is a Authenticated website or Vulnerable website. If the decision is "green", then the url of a website is authenticated and user can communicate with it, Otherwise if the decision is "Red" then the website is not a trustworthy website i.e. it is vulnerable.

TABLE I

LIST OF SITE VALIDATION

URLS	TIME	DECISION	STATUS
https://www.gmail.com/	3.313	GREEN	AUTHENTICATED
https://jntufastupdates.com/	3.225	GREEN	AUTHENTICATED
http://www.google.co.in//	2.58	RED	VULNERABLE
http://www.infosys.com/careers/	2.44	GREEN	AUTHENTICATED
http://www.w3schools.com/php/default.asp//	5.534	RED	VULNERABLE
https://www.google.co.in/	4.234	GREEN	AUTHENTICATED
https://www.sbi.co.in/	2.99	GREEN	AUTHENTICATED
http://www.gmail.com./@	5.05	RED	VULNERABLE
https://www.paytm.in	3.433	GREEN	AUTHENTICATED

The above table 1 maintains a detail description about list of website and its performance is provided to recognize that a particular site is authenticated or vulnerable website based on decision generated by TwoFish approach. Time factor is indicated to every url of webpage to know that how time it takes to validate a website and generate a report to the user. By concerning these time factor we can conclude that this TwoFish approach takes less computation time to validate the website and generate accurate results.

The below bar diagram (Fig 2) makes a clear explanation of TwoFish security approach that notify the computation time for each url i.e. how much time it takes to validate the website based on url.

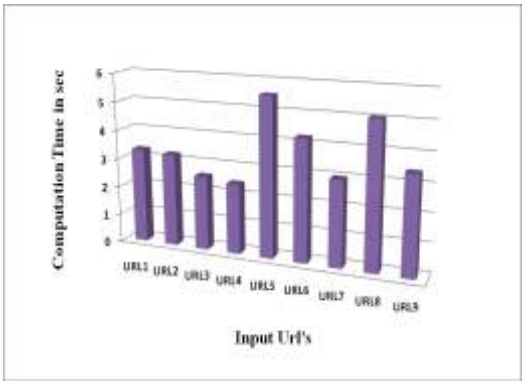

Fig 2: Bar Diagram for TwoFish Security Approach

Based on the above experimental results we observed that TwoFish security approach provides an efficient way to validate any website that means it takes less time for computing the website url and similarity identification of images is also accurate and there is no complexity to the user to verify that a particular site is genuine or vulnerable website.

V. CONCLUSION AND FUTURE SCOPE

As our need on the Internet increases, the attacks related to these dependencies may also increases. We know that phishing attacks are more common in today's technology because it can attack globally and capture the confidential information of users in an undefined manner. One such type of vulnerability is Cross Site Request Forgery (CSRF) attack. It is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts which may leads to loss of confidential data. This type of attack is difficult to detect and prevent. CSRF attacks are occurred because browser authenticates the website, not by the user. We have implemented a novel approach "Avoiding Cross Site Request Forgery Attack Using TwoFish Security approach" is a better way to avoiding the CSRF attacks. This TwoFish security allows the user to validate the website and get decision regarding whether the site is trustworthy or not. This methodology provides authentication in two phases: Firstly it calculates the hash value for URL by using MD5 algorithm and secondly it produces image encryption by which more security is provided to validate the website. By using this strategy, the user can easily recognize whether a particular website is a genuine or vulnerable website and provides service oriented authenticated websites to respective clients, further we can try to implement this application in college level system and test the various security parameters.

REFERENCES

[1] Anjali Jose, S.vinoth lakshmi "Web Security using visual Cryptography against Phising" *Middle East Journal of Scientific Research*, ISSN 1990-9233, 2014.

[2] W. Zeller and E. W. Felten, "Cross-Site Request forgery Forgeries: Exploitation and prevention," technical report,Princeton university, 2008.

[3] Grossman, "Cross Site Request Forgery 'The Sleeping Giant of Website Vulnerabilities'", in RSA Conference, San Francisco, April 2008.
[4] Xiaoli Lin, Pavol Zavarsky, Ron Ruhl, Dale Lindskog,"Threat Modeling for CSRF Attacks", the International Conference on Computational Science and Engineering, 2009.
[5] J.Burns. Cross Site Reference Forgery: An introduction to common web application weakness. www.isecpartners.com/documents/ SRF_ paper.Pdf.
[6] A survey on Cross-Site Request Forgery attack preventive measures to fully exploit the attacks in www.owasp.org.index.php/cross__ site_request_forgery, may,2009
[7] Kombade, Rupali D., and B. B. Meshram. "CSRF Vulnerabilities and Defensive Techniques." International Journal of Computer Network and information Security (IJCNIS) 4.1 (2012): 31.
[8] OWASP. https://www.owasp.org/index.php/top_10 2013_top_10.
[9] Mitchell. RobustDefenses for cross site Request forgery.In.CSS 2008.Feil, Renaud, and Louis Nyffenegger. "Evolution of cross site request Forgery attacks." Journal in Computer Virology 4.1 (2008): 61-71.
[10] APWG, 2006 Origins of the Word 'Phishing'. Define phishing attacks to explore security http://www.antiphishing.org/word_phish.htm
[11] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why phishing works. In Proceedings of the Conference on Human Factors in computing systems (CHI), 2006.
[12] "Phishing Email Filtering Techniques: A Survey" by P.Rohini, K.Ramya, Volume 17, Number 1, Nov-2014, ISSN:2231-2803.
[13] E.W. Felten, D. Balfanz, D. Dean, and D. S. Wallach.Web Spoofing: An Internet Con Game. In *20th National Information Systems Security Conferenc*e, October 1997(p attacks).
[14] D.Geer, "Security Technologies Go Phishing, "Computer Archive, Volume 38, Issue 6, June 2005, pp18-21
[15] "Detecting phishing attacks in purchasing process through pro-active Approach" by the s.arun, D.Anand, T.selvaprabhu, anna university, 2012.
[16] Sun Bin, Wen Qiaoyan and Liang Xiaoying, 2010. A DNS based AntiPhishing Approach, in Proceedings of *IEEE-Second International conference on Networks Security, Wireless Communications and Trusted Computing*.
[17] "A new framework for Thwarting phishing attacks based on Visual Cryptography" by Kamalakar Sanka, Betam Suresh, Volume 4, Issue8 ,August 2013,ISSN: 2231-2803.
[18] CAPTCHA:Using Hard AI problems for security Luis von Ahml, Manuel Blum1,Nicholas J.Hopper1, and John Langford
[19] Anthony, Y. and Fu, Liu Wenyin, October/December 2006. Detecting Phishing Web Pages with Visual Similarity Assessment Based on this Earth Mover's distance (EMD), *IEEE Transactions on Dependable and Secure Computing*, 3(4): 301-311
[20] Tainan Li. Fuye Han, Shuai Ding and Zhen Chen, 2011.LARX: Large scale Anti-phishing by Retrospective Data-Exploring Based on cloud computing Platform, in Proceedings of *IEE-20th International conference on computer communications and network*.
[21] Nirmal, K., S.E.V. Ewards and K. Geetha, 2010. Maximizing online security by providing a 3 factor authentication system to counter-attack phishing Proceedings of IEEE- International Conference on emerging trends in Robotics and Communication Technologies.