International Journal of Scientific Research and Engineering Development-– Volume 3 Issue 2, Mar-Apr 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Defending Phishing Attacks on E-Banking Websites Using Captcha Authentication

N.R Vishnupriya*, P.Vennila**, P.Vinoda***, R.Yogalakshmi ****

*M.E, Assistant Professor, Department of Information Technology, Jeppiaar SRR Engineering College, Padur, Chennai, Tamil Nadu, India

**B.TECH, Department of Information Technology, Jeppiaar SRR Engineering College, padur, Chennai, Tamil Nadu, India

***B.TECH, Department of Information Technology, Jeppiaar SRR Engineering College, padur, Chennai, Tamil Nadu, India

****B.TECH, Department of Information Technology, Jeppiaar SRR Engineering College, padur, Chennai, Tamil Nadu, India

----------**********----------

Abstract:

Phishing is an attempt by an individual or a group to steal personal information such as passwords, credit card information etc from unaware victims for identity theft, financial gain and other fraudulent activities. The first security should be the authentication mechanism in a web application. The username and password based authentication is not enough for websites provide critical financial transactions. We have proposed an approach for phishing websites classification to solve the problem of phishing. Phishing websites contain a variety of signal within its content as well as the browser-based security measures provided along with the website. The use of images is search to preserve the privacy of image CAPTCHA by decay. The original image CAPTCHA into two, shares that are stored in different database servers such that the original image CAPTCHA can be displayed only when both are concurrently available; the individual images do not display the identity of the original image CAPTCHA. Once the original image CAPTCHA is displayed to the user it can be used as the password. Several solutions have been proposed to tackle phishing.

Keywords **— Visual Cryptography Scheme, Validation Scheme, Image captcha Generation, One Time password.**

----------**********----------

I. INTRODUCTION

Online transactions are nowadays become very familiar, and there are various attacks present behind this. In these types of various attacks, phishing is recognize as a major securities threat and new ideas are arising with this in each second so preventive mechanism should also be so strong. Thus, the security in these cases be very high and should not be easily controllable with implementation indifference. Today, most applications are only as secure as their explicit system. Since the design, and technology of middle ware has improved constantly, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not? Phishing fraud are also becoming a problem for online banking and e-commerce users. The question is how to hold applications that require a high level of security. Phishing is a form of online identity fraud that aims to steal responsive

information such as online banking passwords and credit card information from users. Phishing fraud have been receiving extensive press coverage because such attacks have been escalating in number and sophistication. It tries to corrupt acquire responsive information, such as passwords and credit card details, sedate as an honest person or business data communication. The conduct of identity theft with this acquired sensitive information has also become easier with the use of technology and identity fraud can be described as "a crime in which the cheat obtains key pieces of information such as Social Security and driver's license numbers and uses them for his or her own gain." Phishing attacks rely upon a mix of technical scams and social engineering practices. In the majority of cases the phisher must get the victim to intentionally perform a series of actions that will provide access to personal information. Communication channels such as email, web pages, IRC and immediate messaging services are popular. In all cases the phisher must impersonate a trusted source for the victim to believe. To date, the most successful phishing attacks have been initiated by email — where the phisher impersonates the sending authority so here introduces a new method which can be used as a secure way against phishing is named as "A novel approach against Anti-phishing using visual cryptography." As the name describes, in this approach website cross validates its own identity and show that it is an original website to use bank transaction, E-commerce and online booking system, etc. before the end users and make the both the sides of the system secure and a validated one. The concept of image processing and a better visual cryptography is used. Image processing is a technique of processing an input image and to get the output as either better form of the same image or characteristics of the input image. Visual Cryptography (VC) is a method of encrypting a secret image to shares, such that store a sufficient number of shares display the secret image.

II. RELATED WORKS

"Defining Code-Injection [1]", Donald Ray, Jay Ligatti , 2012 This paper shows that existing definitions of code-injection attacks (e.g. SQL-injection attacks) are defects. The defects make it possible for attackers to avoid existing mechanisms, by supplying code-injecting inputs that are not recognized as such. The flaws also make it possible for benign inputs to be treated as attacks. These faults in standard definitions of code-hit attacks, this paper proposes a new definition, which is based on whether the sign input to an application get used as (normal form) values in the application's output. Because values are already fully estimated, they cannot be considered, "code" when injected. This simple definition of code-hit attacks avoids the problems of existing definitions, it improves our understanding of how and when such attacks occur, and enables us to estimate the success of mechanisms for wrath such attacks.

"Run-Time Monitoring And Formal Analysis of Information Flows in Chromium [2]", Lujo Bauer Shaoying Cai , Limin Jia Timothy Passaro Michael Stroucken Yuan Tian, 2015, Web browsers are a key enabler of a vast range of online services, from shopping and email to banking and health services. Because these services frequently involve handling sensitive data, a wide range of web browser security policies and mechanisms have been implemented or proposed to mitigate the dangers posed by malicious code and sites. This paper describes an approach for specifying and enforcing changeable information-flow policies on the Chromium web browser. It focuses on an existing browser and enclose a broad range of browser features, from pages and scripts to DOM elements, events, persevering state, and string out. In our approach, which is a cheap-grained, light-weight execution of fault tracking, entities in the browser are explained with information-flow labels that specify policy and track information flows. We create a detailed formal model of our approach, for which we prove non-interference. We also develop a corresponding

interface system built on top of Chromium. Demonstrate, and experimentally confirm, that the system can enforce many existing browser policies, as well as practically useful policies beyond those legal in standard web browsers.

III. PROPOSED SYSTEM

We have proposed a new approach for phishing websites classification to solve the problem of phishing by adding security in user authentication phase. Phishing websites comprise a variety of sign within its content as well as the browser-based security measures provided along with the website. The use of images is to protect the privacy of image CAPTCHA by decaying the original image CAPTCHA into two, shares that are stored in separate database servers such that the original image CAPTCHA can be displayed only when both are simultaneously convenient ; the individual images do not display the identity of the original image CAPTCHA. Once the original image CAPTCHA is displayed to the user it can be used as the password. To develop the CAPTCHA we have been using the Visual Cryptography technique. Vs is a hidden technique that allows for the encryption of optical information such that decryption can be performed using the human visual system. (2, 2)-Threshold Vs scheme- This is the simplest threshold scheme that takes a confidential message and encrypts it two different shares that display the confidential image when they are concealed. In the case of (2, 2) Vs, each pixel in the original image is encrypted into two sub pixels called shares. Note that the choice of shares for a white and black pixel is made determined (there are two choices available for each pixel). Neither share provides any hint about the original pixel since different pixels in the secret image will be encrypted using independent made choices. When the two shares are imposed, the value of the original pixel P can be determined. If Pixel is a black pixel, we get a two black sub pixels; it is a white pixel, we get one black sub pixel, and one white sub pixel.

IV. SYSTEM DESIGN

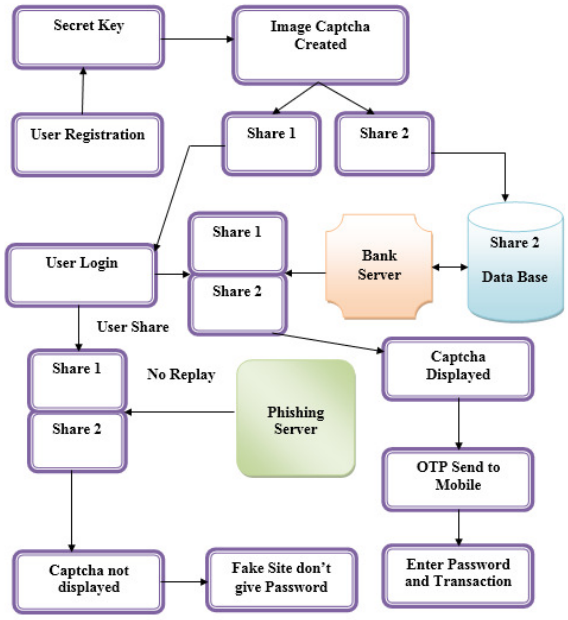

Figure 1: System Architecture

A. *Use case Diagram*

Unified Modelling Language (UML) may be a systematized general-purpose modelling language within the field of software engineering. The standard is managed and was created by the thing Management Group. UML includes a group of graphic representation techniques to make visual models of software intensive systems. This language is employed to specify, imagine, modify, build and document the artifacts of an object-oriented software intensive system under development.

B. *Class Diagram*

A Class diagram shows how the dissimilar entities interconnected to each other in the Unified Modelling Language was a type of static structure diagram that illustrate the structure of a

system by demonstration the system's classes, their attributes, operations (or methods), and the relationships among objects.

C. Collaboration Diagram

UML Collaboration Diagrams illustrate the link and interaction between software objects. They necessitate use cases, system operation contracts and domain model to already exist. The collaboration diagram embellished messages being sent between classes and objects.

D. Sequence Diagram

A Sequence diagram is a kind of interaction diagram that shows how the procedure manages with one another and in what order. It is a build of Message Sequence diagrams are sometimes called event diagrams, event scenarios and timing diagram.

E. Activity Diagram

Activity diagram is a graphical representation of workflows of gradual activities and actions with support for possibility, looping and consistency.

The most important shape types:

- Rounded rectangles represent activities.
- Diamonds represent decisions.
- Bars represent the start or end of consistent activities.
- A black circle represents the start of the workflow.
- An encircled circle represents the end of the workflow.

F. Data Flow Diagram

The Data Flow Diagram is a graphical representation of the “flow” of data through an information system, modelling its point. It is a preliminary step used to create an overview of the system which can later be elaborated Data Flow Diagram can also be used for visualization of data processing.

V. MODULES

A. Registration With Secrete Code

In the registration phase, the user details user name, password, email-id, address, and a key string(password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more safe environment. This string is concatenated with randomly generated string in the server..

B. Image captcha Generation

A key string is converted into image using java classes moderated Image and Graphics 2D. The image capacity is 260×60. Text color is red, and the background color is white. Text face is set by Font class in java. The image creation it will be written into the user key folder in the server using Image IO class.

C. Shares Creation (VCS)

The image CAPTCHA is divided into two shares such that one of the shares is retain with the user, and the other share is kept in the server. The user's share and the original image CAPTCHA sent to the user for later verification during login phase. An image CAPTCHA is also stored in the actual database of any confidential website as confidential data.

D. Login Phase

Allocate initial currencies to the individual conspire utilizing individual gadgets that use

distinctive cryptographic natives, for example, encryption, advanced mark, pixel determination. The profit strategy by the broad utilization of figuring and different smart convenient gadgets that can empower clients to execute a safe verification convention. It keeps static username and secret key tables for distinguishing and confirming the authenticity of the login clients. Furthermore, picture pixel 6789utilizing for to open the record. In the event that we are not pick amend point picture implies the record won't open. It is secure technique.

VI. CONCLUSION

Currently, phishing attacks are so familiar because it can attack globally and capture and store the users' personal information. This information is used by the attackers which are accidentally involved in the phishing process. Phishing websites as well as the users can be easily identified using our proposed, Anti-phishing support based on Visual Cryptography. The proposed methodology preserves confidential information of users. Verifies whether the website is a genuine or secure website or a phishing website. If the phishing website (website that is a fake one just similar to secure website but not the secure website), then in that the phishing website can't display the image CAPTCHA for that specific user (who wants to log in into the website) because the image CAPTCHA is generated by the store of two shares, one with the user and the other with the database of the website. The proposed system is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market.

REFERENCES

[1] N. Jovanovic, E. Kirda, and C. Kruegel, "Preventing cross site request forgery attacks," in Proceedings of the Second International Conference on Security and Privacy in Communication Networks. IEEE Computer Society, 2006.

[2] M. Shahzad, M. Z. Shafiq, and A. X. Liu, "A large scale exploratory analysis of software vulnerability life cycles," in ICSE '12. IEEE Press, 2012, pp. 771–781.

[3] Z. Su and G. Wassermann, "The essence of command injection attacks in web applications," in Proceedings of the 33rd ACM Symposium on Principles of Programming Languages, 2006, pp. 372–382.

[4] D. Ray and J. Ligatti, "Defining code-injection attacks," in POPL '12. ACM, 2012, pp. 179–190.

[5] W. G. Halfond, J. Viegas, and A. Orso, "A classification of SQL-injection attacks and countermeasures," in Proceedings of the International Symposium on Secure Software Engineering, Mar. 2006.

[6] S. Stamm, B. Sterne, and G. Markham, "Reining in the web with content security policy," in Proceedings of the 19th International Conference on World Wide Web, 2010, pp. 921–930.

[7] L. Bauer, S. Cai, L. Jia, P. Timothy, S. Michael, and T. Yuan, "Run-time monitoring and formal analysis of information flows in Chromium," in NDSS '15, 2015.

[8] D. Wagner and P. Soto, "Mimicry attacks on host-based intrusion detection systems," in CCS '02, 2002, pp. 255–264.

[9] G. S. Kc, A. D. Keromytis, and V. Prevelakis, "Countering code-injection attacks with instruction-set randomization," in CCS '03. ACM, 2003, pp. 272–280.

[10] W. G. Halfond and A. Orso, "AMNESIA: analysis and monitoring for neutralizing SQL-injection attacks," in Proceedings of the 20th International Conference on Automated Software Engineering. ACM Press, Nov 2005, pp. 174–183.

