International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Novel Approach to Anti-Phishing Using Visual Cryptography

Sofia Backiya B.[1], Geetha M.[2], Sathya M.[3], Preethika D.[4]

[1, 2, 3, 4] B.E., Computer Science Engineering, Dr. Mahalingam College of Engineering and Technology, Pollachi

Abstract: ***Phishing is a criminal activity, fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal their information such as passwords, credit card number, etc. online. It has always been a simple and effective way to steal the credential of the user mainly on internet banking and e-commerce. All though methods like security image, etc. have been used but they have often proven ineffective. In order to avoid phishing in particular, we have made use of Visual Cryptography at login level on websites to verify its own identity and prove that it is a genuine website before the end users and make both the sides of the system secure as well as an authenticated one. This technique not only allows website to prove its identity but also adds another layer of security on it. This project makes use of Visual Cryptography Schema (VCS) to add an image based security for authentication for both the user and the website. The authentication was achieved by the three layer of checking which includes the password, security code and then the one-time password. The security code and the password will be given by the user during the process of registration. Once this is validated, the one-time password will be sent to the user to their mail ID.***

Keywords: Shares creation, random number generation, Visual cryptographic algorithm, captcha generation, OTP generation

1. Introduction

Nowadays, online transactions have become very common and there are various attacks present behind this. In these types of attacks, phishing is identified as a major security threat and new innovative ideas are arising on a regular basis. This helps to increase the preventive measures.

Phishing is a form of online identity theft that aims to steal sensitive information like online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication.

Thus the security in these cases be very high and should not be easily tractable with implementation easiness. Today, most applications are only as secure as their underlying system. As the design and technology of middleware has improved steadily, 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 scams are also becoming a problem for online banking and e-commerce users. The question is how to handle applications that require a high level of security.

One definition of phishing is given as —it is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. The conduct of identity theft with this acquired sensitive information has also become easier with the use of technology and identity theft can be described as —a crime in which the impostor 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 deceit and social engineering practices. In the majority of cases the phisher must persuade the victim to intentionally perform a series of actions that will provide access to confidential information.

Communication channels such as email, webpages, IRC and instant 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.

2. Existing System

In the existing system data of the user are mostly secured. User name and Password has been used in the past to secure the data from the hackers. As there is no proper way to secure the user data hackers have been using phishing as an easy and effective way to phish the user data resulting in identity theft. There has been use of captcha as a method to stop the robots (malicious code) from stealing the user data. This method has proven effective against the robots but not hackers. As to secure the user data tools like VSI (Visual Security Indicators), SSL warning has been used.

There is no particular algorithm that was followed to generate this system, but it used a method of identifying the authenticated user with a password and a security image. But it was not so effective because most of the people found it annoying to use security images every time they log in.

Many of the major Internet banking websites display a security image and caption each time a user logs into the account as a security measure. When a user first registers for an account, she is prompted to pick a security image from a list of security images as well as to create a caption to accompany the image.

The security image and caption are shown to the user on all subsequent logins, and the user is instructed not to log in if she notices that the image or captions are missing or incorrect. This strategy is believed to help protect users from

Licensed Under Creative Commons Attribution CC BY

phishing attacks: During a phishing attack, a user might be attracted to a fake web site that mimics a real one in all ways except that it does not show the user's chosen security image; a vigilant user might notice the absence of the security image and refuse to log in.

Security images are often used as part of the login process on internet banking websites, under the theory that they can help foil phishing attacks. Previous studies, however, have yielded inconsistent results about user's ability to notice that a security image is missing and their willingness to log in even when the expected security image is absent. This system describes an online study of 482 users that attempts to clarify to what extent users notice and react to the absence of security images.

We also study the contribution of various factors to the effectiveness of security images, including variations in appearance and interactivity requirements, as well as different levels of user motivation. The majority of our participants (73%) entered their password when we removed the security image and caption. We found that features that make images more noticeable do not necessarily make them more effective at preventing phishing attacks, though some appearance characteristics succeed at discouraging users from logging in when the image is absent. Interestingly, we find that habituation, the level of financial compensation, and the degree of security priming, at least as explored in our study, do not influence the effectiveness of security images.

A study by Wu et al. showed the ineffectiveness of security toolbars that displayed security related information which was meant to help users detect phishing attacks. Also, many users do not know about phishing attacks or realize how sophisticated the attacks can be. Another study, by Sunshine et al., tried to redesign existing SSL warnings.

Even though .their warnings performed much better than existing warnings, they found that too many participants continued to exhibit dangerous behavior in all warning conditions. The authors of the paper suggested that the better approach might be to minimize using SSL warnings altogether by preventing users from making unsafe connections or to eliminate warnings in benign situations.

3. System Methodology

A. Goals and Overview

The focus of this system was not just to measure whether security images were effective, but also to examine what makes them effective. For example, we explore the influence of factors such as the size, appearance, and customizability of security images. Also, we wanted to find out whether changes to the way the study was conducted—such as by making participants more security conscious, paying them more for the system, etc.—would cause them to pay more attention to the security images.

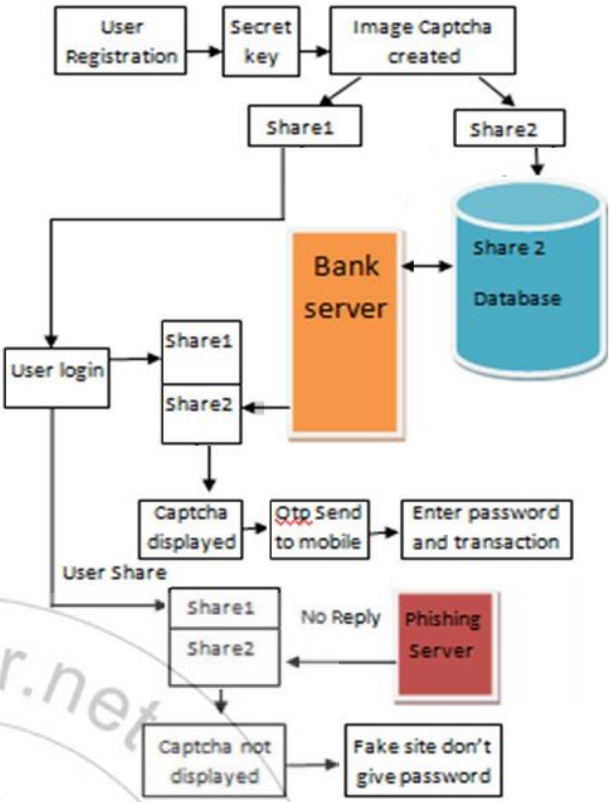

Figure 1: System Architecture

Several of these variations were motivated by the desire to shed light on the divergent results obtained by previous studies. Since the security images were typically displayed on internet banking websites and because we want to examine how users react in a high-value website, we decided to simulate a real-life internet banking scenario.

B. System Procedure

Hereby propose a system with a more protected authentication and several layers of security. This is done with the involvement of an algorithm known as Visual Cryptographic algorithm. It consists of four modules. They are Registration with code along with random number generation, image generation in captcha format from the security code, share image creation using visual cryptography method, login and onetime password (OTP) generation.

The steps are as follows. The first page will be the home page. The second page is the register page, where the user will have to type all the required details that was asked by the server. And then the secret code and the password given by him will be stored in the database and the confirmation of his/her password will be sent to his/her email id.

Then some five digits will be added to this secret code and this as a whole will contribute to the creation of a new image which looks like a captcha. This will be split into two and one share will be given to the user. When the user logs in, he/she can make use of this share to upload it in the login page.

Licensed Under Creative Commons Attribution CC BY

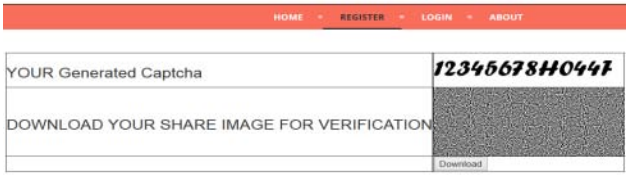

Figure 2: Share Generation

If the shares of the images from the server and the user match, the original image will be displayed. Or else, the image will not be displayed. When the image appears, the One-Time password will be sent to the mobile user mail ID.

Visual cryptographic algorithm - The system involves an automatic segregator of Images which is a two-step process of converting any images into the required Visual cryptography formatted images. After getting the original image, the images will be bifurcated into various shares depends on the access structure.

Shares creation - Visual cryptography (VC) is a modern cryptographic technique which is used to the secret image is shared securely and the information is maintained with utmost confidentiality. A sender transmits the secret image which is divided into multiple shares and it holds hidden information. When all of these shares are aligned and stacked together, they expose the secret image information to the receiver.

C. Survey

The exit survey asked participants to indicate how much they agree or disagree with the following five statements about the security image that they saw each time they logged in.

1) Using a security image as part of the login process was annoying.
3) I wish that my bank's website used a similar security image.
4) I did not look at the security image before I entered my password.
5) Using a security image as part of the login process helps to improve online security.

Participants were asked to indicate their agreement with each statement on a Likert scale with the following five choices: Strongly disagree, Disagree, Neutral, Agree, Strongly agree. We also asked participants six demographics questions about their age group; gender; country; whether they are majoring in or do they have a degree or job in computer science, computer engineering, information technology or a related field; their highest level of education; and if they have done one or more of the following:

- Deleted browser cookies,
- Cleared their web browser cache,
- Changed their web browser cookie policy,
- Refused to give information to a website, or
- Supplied false or fictitious information to a website when asked to register.

4. Results

Currently phishing attacks are very common because it can attack globally and can capture the user's confidential information. Identification of a phishing site is not easy for a common user since it is an identical copy of real website.

Our proposed methodology preserves confidential information of users by verifying the website.

If the website is a phishing website (website that is a fake one just similar to secure website but not the secure website), then in that situation, the phishing website can't display the image captcha for that specific user (who wants to log in into the website) due to the fact that the image captcha is generated by the stacking of two shares, one with the user and the other with the actual database of the website.

The proposed methodology will be useful in identifying the phishing websites on financial web portal, banking portal, online shopping market and other sites which handles sensitive data.

Table 1: Analysis of our system

User Name	*Share 1*	*Share 2*	*Matching Property*
Reeju	Server sharereeju	keyimagereeju	Yes
Rian	Server sharerian	keyimagesarah	No

Table 2: Result of our system

Contents	*Existing System*	*Proposed System*
Security Layers	One	Three
Number of users surveyed	569	602
Percentage of good response	73.03%	77.6% as Effective 12% as Strongly Effective
Time period of Survey	April and May 2013	November and December 2016

5. Future Enhancement

In future we can increase the security by adding many algorithms to encrypt the image. Encryption Phase contains many algorithms like Blowfish, Splitting and Rotating algorithm and (2, 2) Visual Cryptography Scheme.

Another method of barcode scanning can also be done. This can be done directly by giving the user a barcode which can be used by them to log in. The user can use the barcode scanner application for this purpose. This will be merged with our system, which will be easier and effective.

Many new methods can be added like hiding the secret code inside an image using the steganography method. This can be done to replace the one-time password system. This will not help the hackers to find the code easily.

References

[1] Chetana Hedge, S Manu, P DeepaShenoy, K R Venugopal, L M Patnaik. —Secure Authentication Using Image-Processing And Visual Cryptography for

Licensed Under Creative Commons Attribution CC BY

Banking Applications(2008)‖ 16th International Conference on 14-17 December 2008
[2] IJ Cox, J Kilian, FT Leighton, T. Sharmoon. —Secure Spread Spectrum Water Marking for Multimedia (1997) Volume: 6 Issue: 12.
[3] Feng Liu, Chuakan Wu, Xijun Lin. —Step Construction of Visual Cryptography Schemes‖ IEEE Transactions on Information Forensics and Security 2010
[4] Geum-Dal Park, Eun-Jun Yoon, Kee-Young Yoo. —A New Copyright Protection Scheme with Visual Cryptography‖ Future Generation Communication 2008
[5] N. Gowdham, S.D. Libin Raja, M. Sornalakshmi, M. Navaneetha Krishnan(2014) Two Step Share Visual Cryptography Algorithm for Secure Visual Sharing — National Journal on Recent and Innovation Trends in Computing and Communication Volume: 2 Issue: 3.
[6] Joel Lee, Lujo Bauer, Michelle L. Mazurek(2015) Studying the Effectiveness of Security Images in Internet Banking', DOI 10.1109/MIC.2015.108, IEEE Transactions on Internet Computing.
[7] Jonathan Weir, WeiQi Yan. —Sharing Multiple Secrets Using Visual Cryptography‖ IEEE International Symposium on 24-27 May 2009
[8] Joseph James S, Rajan S (2011) Enhanced Color Visual Secret Sharing Scheme using Modified Error Diffusion' ICRTCT
[9] Joshua Sunshine, Serge Egelman, HazimAlmuhimedi, NehaAtri, Lorrie Faith Cranor (2009) Crying Wolf: An Empirical Study of SSL Warning Activeness' USENIX Security Symposium, pp. 399-416.
[10] Min Wu, Robert Miller .C, Simon Garfield .L (2006) Do Security Toolbar Actually Prevent Phishing Attack', CHI.
[11] Pei-Ling Chiu, Risk Management and Insurance, Ming Chuan University, Taipei, R.O.C, Kai-Hui Lee, Dept., of Computer Science and Information Engineering, Taipei, R.O.C. —A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes(2014) Volume : 6 Issue : 3
[12] P.S. Revenkar, AnisaAnjum, W. Z. Gandhare. —Secure Iris Authentication Using Visual Crptography Submitted on 10 April 2010
[13] T. Stojanovski, L. Kocarev. —Chaos-Based Random Number Generators-part I: analysis[cryptography] IEEE Transactions on Circuits and Systems, 07 August 2002
[14] T. Stojanovski, J. Pihl, L. Kocarev. —Chaos-Based Random Number Generators-part II: practical realization‖ IEEE Transactions on Circuits and Systems, 07 August 2002. Volume : 48 Issue : 3
[15] Wen-Bin Hsieh, Jenq-ShiouLeu. —Design of a Time and Location Based One-Time Password Authentication Scheme‖ Wireless Communications and Mobile Computing Conference(IWCMC), 2011 7th International Conference 12 August 2011
[16] Xiaoyu Wu, Duncan S. Wong, and Qing Li. —Threshold Visual Cryptography Scheme for Color Images with No Pixel Expansion‖ Proceedings of the Second Symposium International Computer Science and Computational Technology,26-28 Dec, 2009.
[17] Yinian Mao, ECE Dept., Maryland Univ., College Park, MD, USA, Min Wu, ECE Dept., Maryland Univ., College Park, MD, USA. —Security Evaluation for Communication-Friendly Encryption of Multimedia‖ ICIP '04. 2004 International Conference on 24-27 October 2004

Licensed Under Creative Commons Attribution CC BY