The Effectiveness of Security Images in Internet Banking

[1]Jebakumar Immanuel.D, [2]Ranjani.G, [3]Nandhini.V, [4]Shanmugha Priya.R
Assistant Professor [1], UG Scholar [2],[3],[4]
Department of Computer Science and Engineering, SNS College of Engineering, Coimbatore

Abstract

Security images are again used as part of the login process on internet banking websites,under the theory that they can help to find the phishing attacks in the websites.The majority of our participants entered their password when we removed the image and captcha. We found changing the appearance and other characteristics of the security image generally had little effect on whether user logged in when the security image was absent.Additionally we subjected the passwords are created by users to a password cracking algorithm and found that participants with stronger passwords were less likely to enter their password when the security image was missing.

I. INTRODUCTION

As a secure image measure, many banking websites shows a security image and caption each time a user logs into the account. When a user first registers for an account, she is prompted to pick a security image from a list of available images as well as to create a caption to escort the image. The security image and caption are shown to the user on all succession logins, and the users are not instructed to log in if she notices that the image or caption are missing or incorrect. This strategy is believed to help protect users from phishing attacks: If a phishing web site mimics a real one in all the ways of expectations that it does not show the user's chosen security image, a vigilant user might notice that the absence of the security image and refuses to log in.

II. LITERATURE SURVEY

A. *Human-Seeded Attacks and Exploiting Hot-Spots In Graphical Passwords*

Although motivated by both usability and the security concerns, the existing literature on click-based graphical password schemes using a single background image has focused largely on usability. We examine the security of such schemes, including the collision of different background images, and approach for guessing user passwords. We report on both short- and long-term user studiesone lab controlled, involving 55 users and 17 diverse images, and the other a field test of 223 user accounts. We provide evidence that popular points already exist for many images, and explore two different types of attack to exploit this hotspotting a "human-seeded" attack based on harvesting click-points from a small set of users, and an entirely different automated attack based on image processing techniques.Our most effective attacks are generated by harvesting password data from a small set of users to attack other targets. These attacks can guess 40% of user passwords within 321 guesses inone instance, and 35%within 323 guesses in a second instance. We perform an image-processing attack by implementing and adapting a bottom-up model of visual attention, resulting in a purely automated tool that can guess up to 25% of user passwords in 225 guesses for some instances, but under 4% on others. Our results suggest that these graphical passwordand schemes appear to be at least as susceptible to offline attack as the traditional text passwords they were proposed to alter.

B. *Journey of Vcs from Black and White Images*

Visual Cryptography(VC), an emerging technology for secret sharing which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human vision system(HVS).Originally it was proposed by Naor and Shamir in 1994 for black and white images. Later this technique is extended for gray level images as well as for color images. This paper compares and analyze the performance of various VCS on various parameters such as pixel expansion, contrast, shares generated etc. The compared algorithms came into aura by rectifying limitations of one another.

C. *Visual Secret Sharing*

In the existing random grids based (n, n) visual secret sharing (VSS) schemes, decryption is done with the help of human visual system by stacking the cipher grids. The stacking operation is computationally modeled as Boolean OR operation, which suffers from two drawbacks. Firstly, the contrast of the reconstructed image decreases exponentially by increasing n ($\geq$2) and secondly, it requires perfect alignment of stacking the cipher grids. In this paper, we propose Boolean XOR operation as decryption operation for the existing random grids based (n, n) VSS schemes. The proposed operation removes both the drawbacks and does lossless secret reconstruction. We have demonstrated the improvement in the contrast of the reconstructed image by formal proofs and experimental results.

D. Visual Cryptography Scheme for Secret Hiding:

Visual Cryptography is based on cryptography where *n* images are encoded in a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all shares are stacked together. This paper presents an improved algorithm based on Chang's and Yu visual cryptography scheme for hiding a colored image into multiple colored cover images. This scheme achieves lossless recovery and reduces the noise in the cover images without adding any computational complexity. This paper presented a new technique based on Chang et al. algorithm to hide a color secret image into multiple colored images. The generated camouflage images contain less noise compared to the ones previously obtained using the original Chang's embedding algorithm. This results in a considerable improvement in the signal to noise ratio of the camouflage images by producing images with similar quality to the originals. An improvement in signal to noise ration of 9.3 dB and 19.97 dB were obtained for the initial camouflage images used for hiding the secret image. This developed method does not require any additional cryptographic computations and achieves a lossless recovery of the secret image. In addition, the camouflage images obtained using the modified algorithm look less susceptible of containing a secret message than the ones obtained using the original method.

E. Visual Secret Sharing Scheme:

In this paper a new visual cryptography scheme is proposed for hiding information in images which divide secret images into multiple shares. Secret information can be retrieved by stacking any k number of decrypted shares. This paper introduces the novel method of visual information pixel synchronization (VIP) and Modified threshold error diffusion to attain a color visual cryptography encryption that produces meaningful color shares with high visual quality. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channels and error diffusion generates shares pleasant to human eyes. Error diffusion method uses modified threshold value to improve the quality of shares and decrypted secret image. This paper also uses edge sharpening filters to enhance the edges of images.it introduces a new encryption method to construct color EVC scheme with VIP synchronization and modified threshold error diffusion for visual quality improvement. VIPs synchronize the positions of pixels that carry visual information of original images across the color channels to retain the original pixel values before and after encryption. Modified threshold Error diffusion is used to construct the shares such that the noise introduced by the present pixels is diffused away to neighbours when encrypted shares are generated and optimizes the halftone process to improve the quality of encrypted shares and decrypted secret image. In addition, the use of edge sharpening filter further enhances the image quality.

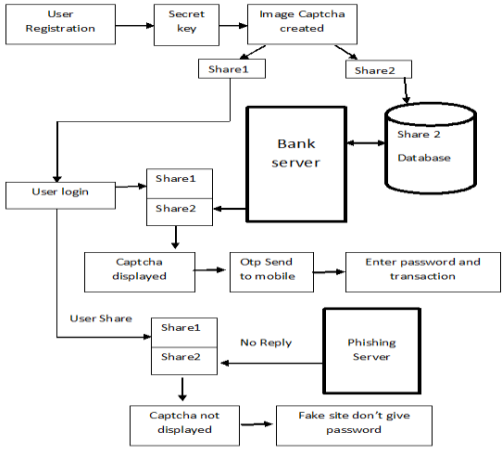
F. Secure Two-Party Computation:

Cryptography is a wonderful world created by humans for serious and noble reasons, populated by many inanimate actors: goals, which are conceptualized and formalized, often in terms of randomized functionalities, in order to treat them properly; basic tools and techniques, which can be used to cope with the different issues an adversarial environment gives rise to when a functionality need to be realized, and protocols, which implement a well-defined communication and computational multi-party strategy to achieve the target goal, i.e., compute a certain functionality. Other actors are definitions and proofs, which are the usual linguistic, logical and mathematical constructs through which functionalities and tools are precisely stated and presented, and protocols are shown to achieve the functionalities for which they are designed in an adversarial model. Research papers often use all of them but, sometimes, some actors are missing, or do not play the roles they deserve. Depending on the contribution the paper provides to the papers could be categorized in different ways: in some papers creativeness, intuition and new ideas are the main components; in others, generalization, abstraction, or sound and rigorous formalization of ideas introduced in a rough or partial form before take the greatest part, while in others, optimization, refinement, and efficiency improvements of protocols, tools and techniques, are the main features. Papers might also be categorized according to the impact on the real world, i.e., if they provide a valuable technological transfer, or to the theoretical Advancement to the field they bring with them. Nevertheless, some papers might just use some of the above actors for intellectual or aesthetic pleasure: neither technological transfer nor theoretical advancement (at least immediately) are provided. However, they might be a useful tool in divulgation activities, and in preparing simple and intriguing presentations of more complex ideas for a general audience. The current paper, perhaps, is (partially) a representative of the last class of papers.

III. ARCHITECTURE DIAGRAM:

First user registered the entire details, it will stored into a database and creating a secret key.After registration process, they give a secret key. If it is correct, the image captcha is generated. The image captcha is splits into 2 shares. Share 1 is having by the user and share 2 is stored into a bank server. If the user wants to login, they give a share1 image to the bank server .Then validation process, the share1 image is

matching to the bank server , the OTP password is send to the users mobile.The user entered the correct password and proceed the transaction process, the image captcha is displayed. If the user having only share1 image, cannot access the sites and the server is not displayed the captcha image.



IV. PROPOSED SYSTEMS

Our method introduce a new method of secure images in the internet banking through online.there are several modules:

1)Registrationwith secret code
2)image captcha generation
3)shares creation(vcs)
4)login phase

V. SYSTEM IMPLEMENTATION

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 secure 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 BufferedImage and Graphics2D. The image dimension is 260*60.Text color is red and the background color is white.Text font is set by Font class in java.After image generation it will be write into the userkey folder in the server using ImageIO class.

C. Shares Creation(Vcs):

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

D. Login Phase:

When the user logs in by entering his confidential information for using his account, then first the user is asked to enter his username (user id).Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user.Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website.

VI. CONCLUSION

It is a real time project which is useful for the user who are facing problem with the phishing websites. This proposal will give the secure image login phase for the online internet banking websites.

REFERENCE

[1] J. Kirk, "Study: Users ignore bank security features," Computerworld, Feb. 2007, http://www.computerworld.com/s/article/9010283/.

[2] Bank of America, "SiteKey FAQs," https://www.bankofamerica.com /privacy/faq/sitekey-faq.go, 2013.

[3] PNC, "Online security information," https://www.pnc.com/webapp/un sec/Solutions.do?siteArea=/pnccorp/PNC/Security+Information, 2013.

[4] Santander Bank, "SSA makes online banking even more secure," https://www.santanderbank.com/us/personal/banking/online-and-mobile-banking/security-center/ssa-learn-more, 2014.

[5] S. Schechter, R. Dhamija, A. Ozment, and I. Fischer, "The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies," in Proceedings of the 28thIEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2007,

[6] A. Herzberg and R. Margulies, "Forcing Johnny to login safely," in

[7] Proceedings of the 16th European Symposium on Research in Computer Security, Leuven, Belgium, 2011, pp. 452–471.