ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
www.ijptonline.com
Review Article

A SURVEY ON APPROACH FOR IMPROVING ANTI-PHISHING SECURITY USING VSS SCHEME IN VISUAL CRYPTOGRAPHY

[1*]Animesh Mukherjee[2], V.Deeban Chakravarthy
[1]PG student, CSE department, SRM University, Kattankulathur.
[2]Assistant Professor, CSE department, SRM University, Kattankulathur.
Email: animeshmkhrj@gmail.com

Received on 10-11-2016 *Accepted on: 28-11-2016*

Abstract:

Phishing is a try by an individual or a social occasion to take singular private information. New approach for phishing destinations gathering to deal with the issue of phishing. Security of trustee based affirmations is used. Phishing destinations incorporate a collection of prompts inside its substance. Program based security markers gave. Special picture captcha into two shares that are secured in confined database servers. Once the principal picture captcha is revealed to the customer it can be used as the mystery key.

Keywords: Image, Generate captcha, cryptography

1. Introduction:

Online exchanges are these days turn out to be extremely basic and there are different assaults exhibit behind this. In these sorts of different assaults, phishing is recognized as a noteworthy security danger and new imaginative thoughts are emerging with this in every second so preventive component ought to likewise be so successful. In this way the security in these cases be high and ought not be effectively tractable with execution effectiveness. Today, most applications are just as secure as their basic framework. Since the outline and innovation of middleware has enhanced relentlessly, their identification is a troublesome issue. Accordingly, it is about difficult to make sure whether a PC that is associated with the web can be viewed as dependable and secure or not. Phishing tricks are likewise turning into an issue for internet managing an account and e-business clients. The question is the manner by which to handle applications that require an abnormal state of security. Phishing is a type of online wholesale fraud that means to take delicate data, for example, internet saving money passwords and charge card data from clients. Phishing tricks have been accepting broad squeeze

scope in light of the fact that such assaults have been heightening in number and advancement. One meaning of phishing is given as "it is a criminal action utilizing social designing systems. Phishers endeavor to falsely obtain touchy data, for example, passwords and charge card subtle elements, by taking on the appearance of a dependable individual or business in an electronic correspondence". The direct of wholesale fraud with this procured delicate data has additionally gotten to be less demanding with the utilization of innovation and fraud can be depicted as "a wrongdoing in which the impostor acquires key bits of data, for example, Social Security and driver's permit numbers and uses them for his or her own pick up". Phishing assaults depend upon a blend of specialized trickery and social designing practices. In the larger part of cases the phisher must induce the casualty to purposefully play out a progression of activities that will give access to secret data. Correspondence channels, for example, email, pages, IRC and texting administrations are mainstream. In all cases the phisher must imitate a trusted hotspot for the casualty to accept. To date, the best phishing assaults have been started by email – where the phisher mimics the sending power

So here presents another strategy which can be utilized as a protected path against phishing which is named as "A novel approach against Anti-phishing utilizing visual cryptography ". As the name delineates, in this approach site cross checks its own personality and demonstrates that it is a veritable site (to utilize bank exchange, E-trade and web booking framework and so on.) before the end clients and make the both the sides of the framework secure and in addition a verified one. The idea of picture handling and an enhanced visual cryptography is utilized. Picture handling is a strategy of preparing an information picture and to get the yield as either enhanced type of the same picture and/or qualities of the information picture. Visual Cryptography (VC) is a strategy for scrambling a mystery picture to shares, to such an extent that stacking an adequate number of shares uncovers the mystery picture.

2. Literature Survey:

[1]Robert Biddle, Sonia Chiasson, P.C. van Oorschot was used to Graphical Passwords: Learning from the First Twelve Years. Starting around 1999, a great many graphical password schemes have been proposed as alternatives to text-based password authentication. We provide a comprehensive overview of published research in the area, covering both usability and security aspects, as well as system evaluation. The paper first catalogues existing approaches, highlighting novel features of selected schemes and identifying key usability or security advantages. We then review usability requirements for knowledge-based authentication as they apply to graphical passwords, identify security threats that such

systems must address and review known attacks, discuss methodological issues related to empirical evaluation, and identify areas for further research and improved methodology.

[2]Alain Mayer, Fabian Monrose, Michael K. Reiter used to The Design and Analysis of Graphical Passwords. In this paper we propose and evaluate new graphical password schemes that exploit features of graphical input displays to achieve better security than text-based passwords. Graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur, and we show that this decoupling can be used to generate password schemes with substantially larger (memorable) password spaces. In order to evaluate the security of one of our schemes, we devise a novel way to capture a subset of the memorable" passwords that, we believe, is itself a contribution. In this work we are primarily motivated by devices such as personal digital assistants (PDAs) that graphical input capabilities via a stylus, and we describe our prototype implementation of one of our password schemes on such a PDA, namely the Palm PilotTM

[3]Susan Wiedenbecka, Jim Watersa, Jean-Camille Birget, Alex Brodskiyc, NasirMemonc used to PassPoints: Design and longitudinal evaluation of a graphical password system. Computer security depends largely on passwords to authenticate human users. However, users have difficulty remembering passwords over time if they choose a secure password, i.e. a password that is long and random. Therefore, they tend to choose short and insecure passwords. Graphical passwords, which consist of clicking on images rather than typing alphanumeric strings, may help to overcome the problem of creating secure and memorable passwords. In this paper we describe Pass Points, a new and more secure graphical password system. We report an empirical study comparing the use of Pass Points to alphanumeric passwords. Participants created and practiced either an alphanumeric or graphical password. The participants subsequently carried out three longitudinal trials to input their password over the course of 6 weeks. The results show that the graphical password users created a valid password with fewer difficulties than the alphanumeric users. However, the graphical users took longer and made more invalid password inputs than the alphanumeric users while practicing their passwords. In the longitudinal trials the two groups performed similarly on memory of their password, but the graphical group took more time to input a password. [4]P.C. van Oorschot, Julie Thorpe used to On Predictive Models and User-Drawn Graphical Passwords. In commonplace text-based password schemes, users typically choose passwords that are easy to recall, exhibit patterns, and are thus vulnerable to brute-force dictionary attacks. This leads us to ask whether other types

of passwords (e.g., graphical) are also vulnerable to dictionary attack due to users tending to choose memorable passwords. We suggest a method to predict and model a number of such classes for systems where passwords are created solely from a user's memory. We hypothesize that these classes define weak password subspaces suitable for an attack dictionary. For user-drawn graphical passwords, we apply this method with cognitive studies on visual recall. These cognitive studies motivate us to define a set of password complexity factors (e.g., reflective symmetry and stroke-count), which define a set of classes. To better understand the size of these classes, and thus how weak the password subspaces they define might be, we use the "Draw-A-Secret" (DAS) graphical password scheme of Jermyn et al. (1999) as an example. We analyze the size of these classes for DAS under convenient parameter choices, and show that they can be combined to define apparently popular subspaces that have bit-sizes ranging from 31 to 41 – a surprisingly small proportion of the full password space (58 bits). Our results quantitatively support suggestions that user-drawn graphical password systems employ measures such as graphical password rules or guidelines, and proactive password checking.

[5]Ahmet Emir Dirik, Nasir Memon, Jean-Camille Birget used to Modeling user choice in the PassPoints graphical password scheme. We develop a model to identify the most likely regions for users to click in order to create graphical passwords in the PassPoints system. A PassPoints password is a sequence of points, chosen by a user in an image that is displayed on the screen. Our model predicts probabilities of likely click points; this enables us to predict the entropy of a click point in a graphical password for a given image. The model allows us to evaluate automatically whether a given image is well suited for the PassPoints system, and to analyze possible dictionary attacks against the system. We compare the predictions provided by our model to results of experiments involving human users. At this stage, our model and the experiments are small and limited; but they show that user choice can be modeled and that expansions of the model and the experiments are a promising direction of research.

[6]Julie Thorpe and P.C. van Oorschot used to Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords Although motivated by both usability and security concerns, the existing literature on click-based graphical password schemes using a single background image(e.g., PassPoints) has focused largely on usability. We examine the security of such schemes, including the impact of different background images, and strategies for guessing user passwords. We report on both short- and long-term user studies: one lab-controlled, involving 43 users and 17 diverse images, and the other a field test of 223 user accounts. We provide empirical evidence that popular points (hot-spots) do exist for many

images, and explore two different types of attack to exploit this hotspotting:(1) a "human-seeded" attack based on harvesting click-points from a small set of users, and (2) an entirely 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 36% of user passwords within 231 guesses (or 12% within 216 guesses) in one instance, and 20% within 233 guesses (or 10% within 218 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 30% of user passwords in 235 guesses for some instances, but under 3% on others. Our results suggest that these graphical password schemes appear to be at least as susceptible to offline attack as the traditional text passwords they were proposed to replace.

3. Summary

VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. We can achieve this by one of the following access structure schemes.

(2, 2)- Threshold VCS scheme- This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid.

Algorithm & Technique

Grayscale conversion: The Captcha image first converts into grayscale using luminance method.

Luminosity:

The gray level will be calculated as

Luminosity = $0.21 \times R + 0.72 \times G + 0.07 \times B$

Vcs Scheme:

In the case of (2, 2) VCS, each pixel P 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 randomly determined (there are two choices available for each pixel). Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices.

When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel.

4. Conclusion

Currently phishing attacks are so common because it can attack globally and capture and store the users' confidential information. This information is used by the attackers which are indirectly involved in the phishing process. Phishing websites as well as human users can be easily identified using our proposed "Anti-phishing framework based on Visual Cryptography". The proposed methodology preserves confidential information of users. verifies whether the website is a genuine/secure website or a phishing 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 is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market. This application can be implemented for all kinds of web application which needs more security.

References

1. R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surveys*, vol. 44, no. 4, 2012.
2. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th USENIX Security Symp.*, 1999, pp. 1–15.
3. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *Int. J. HCI*, vol. 63, pp. 102–127, Jul. 2005.
4. P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawn graphical passwords," *ACM Trans. Inf. Syst. Security*, vol. 10, no. 4, pp. 1–33, 2008.
5. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in Proc. Symp. Usable Privacy Security, 2007, pp. 20–28.
6. J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in *Proc. USENIX Security*, 2007, pp. 103–118.

Corresponding Author:
Animesh Mukherjee*,
Email: *animeshmkhrj@gmail.com*