ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

Prevention of Phishing using Click Points

Kavitha T[1], Ms.S.Vinoth Lakshmi[*2]

[1] Assistant Professor, Department of Information Technology, Jerusalem College of Engineering, Chennai, India

[2*] Assistant Professor , Department of Information Technology, Bharath University, Chennai, India

ABSTRACT: The aim of preventing phishing attack is to find a new authentication technique to protect website from phishing attacks using click points. An attacker can feasibly capture the victim's credentials by fraudulent process. The main goal of phishing is aimed at reducing the effectiveness of phishing attacks that are becoming increasingly problematic for Internet users, based on the traditional username and password paradigm. This is done by providing the user with dynamic display feedback as they enter their passwords, allowing users to stop entering their password that they do not recognizes a sure sign of interacting with the wrong site. This graphical password Click Points describes a security technique enabled with more effective credentials that overcome that deficiency. This will provide a user with security and prevent the disclosure of his/her entire password from phishers.

KEYWORDS: Graphical password, Authentication, Stego-Image, Password security, Cued Click Points

I INTRODUCTION

The word phishing initially emerged in 1990's. The early hackers often use 'ph' to replace 'f' to produce new word hack by phones. Phishing is a new word produced from 'fishing', it refers to the act that the attacker allure users to visit a faked website by sending them faked e-mails (or instant messages), and stealthily get victims personnel information such as username, password.etc. Phishing attacks rely upon a mix of technical deceit and social engineering practices.

The rapid rise of Phishing attacks and their potential to have large negative effects on e-commerce has resulted in a significant number of researchers trying to solve the Phishing problem. The approaches have varied widely, which has appropriately given the fact that Phishing is heart a social engineering attack, and thus on many different guises. This report briefly reviews some of the main works in this area.

Phishing is the criminal activity of enticing people into visiting websites that impersonate the real thing, to dupe them into revealing passwords and other credentials, which will later be used for fraudulent activities. Ideally, the research [2], [3] has attempted to count that Bank of America's website is one of several that users to select a personal image, and display this user-selected image with any forms that request a password. Users of the bank's online services are instructed to enter a password, only when they see the image they selected. However, a recent study suggests few users refrain from entering their password when images are absent. Unlike the website-based image schemes, the image itself is shared only between the user and the browser, and not between the user and the website. This is typically carried out by e-mail or instant messaging [17], and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

In terms of the social engineering aspect [10], it is worth nothing that most of today's Phishing attempts try to make victims give out personal information by intimidating users and creating fear. It should be emphasized that preventing such attacks is an important step towards defending against Phishing attacks. A common Phishing attack is for an attacker to obtain a victim's authentication information corresponding to one website (that is corrupted by the attacker) and then use this at another site. This is a meaningful attack given that many computer users reuse passwords-whether in verbatim in or with only slight modifications. A technique based on this type of attack was proposed, and relies on local and automated scrambling of passwords on a site-by-site basis, performed by a plug-in. Another recent and promising approach [18] detects certain common attack instances, such as attacks in which the images are supplied from one domain while the text resides with another domain, and attacks corresponding to misspellings of URLs of common targets.

A typical Phishing attack begins with an email to the victim, supposedly from a reputable institution, but actually from the phishers. The text of the message commonly warns the user that a problem exists with the user's account that

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

must immediately be corrected. The victim is led to a fraudulent website designed to resemble the institution's official website. At this point, the Phishing site may launch a passive or an active attack. In a passive attack, the web page prompts the victim to enter account information (e.g., username and password) and web page also request other personal details, such as the victim's Social Security Number, bank account numbers, ATM PINs etc. All of this information is relayed to the Phishers, who can then use it plunder the user's accounts. In an active attack, the Phishers may act as a man-in the-middle attacker, actively relaying information from the legitimate site to the user and back. A Universal Man-in-the-middle Phishing kit [9], discovered by RSA Security, provides a simple-to-use interface that allows a phishers to convincingly reproduce websites and capture log-in details entered at the fake site. As a more general form of advanced attack, Jakobsson [10] introduces the notion context-aware Phishing in which an attacker exploits some knowledge about the victim in order to enhance the efficacy of the attack. To defend against Phishing attacks, organizations are in a constant race to detect and take down Phishing sites. In the future, this could become even more difficult with distributed Phishing attacks [11], where each page a user visits is hosted at a different location and registered to a different owner.

Ideally, if the user arrives at a malicious website, he or she will detect that the Phishing site is not the correct website. Jakobsson [10] presents a theoretical framework for Phishing attacks. He also proposes better email authentication to prevent Phishing email, in addition to better secrecy protection for user email addresses (such that Phishers have a harder time harvesting email addresses from, for example, eBay). The Petname project associates a user-assigned nickname with each website visited. If the browser loads a page from a spoofed website, the nickname will be missing or wrong-the approach relies on users to notice either case. In addition, users will likely choose predictable nicknames (e.g., nicknaming Amazon. com's website "Amazon"), making nicknames easy to spoof.

Dhamija and Tygar propose Dynamic Security Skins (DSS) to enable a user to authenticate the server [6], [7]. In their system, a server opens a user-customized popup window that displays an image, only the correct server can produce and then user to perform the verification. Myers [16] proposes that servers display a series of images as users type their passwords. [1] The server also fails to notice the absence of their correct feedback images. Similarly, Pass Mark stores a secure cookie on the client and sets up an image associated with the account that the user should remember. Unfortunately, Pass Mark is a propriety system – they do not disclose a detailed description of their approach. These highly customized attacks, dibbed spear-Phishing, often try to trick employees into installing malware or revealing their organizational passwords [15]. However, this approach would be deployed for websites requiring a high level of security, and that it would ultimately help in regaining victim's confidence in using web-based commerce.

II SYSTEM DESIGN

This section considers the following modules for phishing prevention, in order to provide more security to user credentials before entering into website.

- Cryptosystem
- Steganography
- Cued Click Points
- Watermarking

III MODULE DESCRIPTION

The description of these modules will be discussed briefly under the following sections.

1 Cryptosystem

Data communication is an important aspect of our living. So, protection of data from misuse is essential. A cryptosystem defines a pair of transformations called encryption and decryption. Encryption is applied to the plain text i.e. the data to be communicated to produce ciphertext. Decryption uses the decryption key is the same or one can be derived from the other (i.e. plaintext) then it is said to be symmetric cryptography. The user will generate a pair of related keys one for encryption and other for decryption. One key, which is called the private key, is kept secret and other one known as public key is disclosed. [2]

The username is encrypted with public key and can only be decrypted by using the private key. So, the encrypted username cannot be decrypted by anyone who knows the public key and thus secure communication is possible.[3] RSA (named after its authors Rivest, Shamir and Adleman) is the most popular public key algorithm. In relies on the

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

factorization problem of mathematics that indicates that given a very large number it is quite impossible in today's aspect to find two prime numbers whose product is the given number

In prevention of phishing, first the user gives the username to enter login details in website. In order to provide security, the username is encrypted in the user side and this is sent to server. The encrypted username is embedded in stego-image. Server will retrieve the username by decrypting the cipher text from stego-image. The database will contain all user information's, which is in the form of bytes. So that SQL injection is prevented. Therefore this algorithm is more secured and intruders are unable to retrieve the original username due to this encryption and decryption process.

1.1 RSA Algorithm: RSA (Rivest, Shamir, Adleman) is a popular asymmetric key encryption standard. The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. The key size ranges between 512 and 2048 bits. It is used in many e-commerce applications.

Generally this algorithm makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the blocks size must be less than or equals to $\log_2$ (n). Encryption and Decryption are of the following form, for plaintext blocks M and ciphertext blocks C:

$M=C^d \pmod n$, where $M<n$

$C=M^e \pmod n$

RSA ensures only responsible people are provided to access important data. Therefore this algorithm provides more privacy and reliability to user credentials.[4]

2 Steganography

The word steganography comes from the Greek *Steganos*, which mean covered or secret and *–graphy* mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspect the existence of the message.[6] Hence, secret information is encoded in a manner such that the very existence of the information is concealed and paired with existing communication methods, steganography can be used to carry out hidden exchanges.[7]

This steganography technique, does not alter the structure of the secret message, but hides it inside an original image so it cannot be seen. A message in ciphertext, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists.

It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting *stego-image* can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique and detect the message from the secret message, he would still require the cryptographic decoding key to decipher the encrypted message [4].

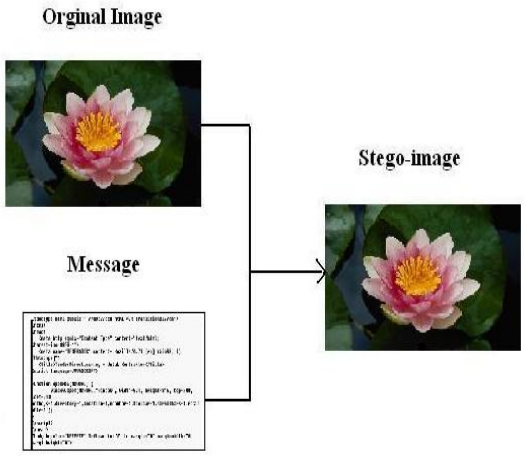

Figure 1. Example of producing Stego-Image process

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

The main goal of Steganography is to hide the secret message and communicate securely in a completely undetectable manner [5] and to avoid drawing suspicion to the transmission of a hidden data. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. The idea of steganography is to keep others from thinking that the information even exists and not to keep others from knowing the hidden information.[8] If a steganography method causes anybody to suspect there is secret information in a carrier medium, then the method has failed. Cryptography can also provide authentication for verifying the identity of someone or something. The purpose of Cryptography and Steganography is to provide secret communication. Cryptography hides the content of a secret message from malicious people, whereas Steganography even conceals the existence of the message[9].

2.1 Least Significant Bit: The steganographic technique focuses on the Least Significant Bit (LSB), in order to hide messages in an image file. LSB defines modifying the rightmost bit in each pixel by replacing it with a bit from the secret message. Least significant bits insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the original image in a deterministic sequence. [10]

For embedding the data into an image, two important files are required. The first is the original image, which will hold the hidden information. The second file is the message itself, which is the information to be hidden in the image. In this process, we decided to use a plaintext as the username.[11] Before embedding process, the size of image and the message must be defined by the system. This is important to be ensuring the image can support the message to be embedded. For example, the ideal image size is 100 × 75 pixels, which can embed up to 15kB messages. After embedding, the original image will be combined with the message. This will produce the output called *stego-image*, which is shown in Fig. 1. The Stego-image seems identical to the original image.[12] Steganography is combined with cryptography, which enables people to communicate without possible eavesdroppers. The methods used in the science of steganography have advanced a lot over the past centuries, especially with the rise of the computer era. This will lead us to define the best approach of steganography to hide information's in phishing prevention.[13]

3 Cued Click Points

To identify the most likely regions for users to click in order to create a Click-based graphical passwords scheme called *Cued Click Points (CCL)* as shown in Fig. 2. A password consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. Cued Click Point can be viewed as a combination of *PassPoints*. A PassPoints is a sequence of points, chosen by a user in an image that is displayed on the screen.

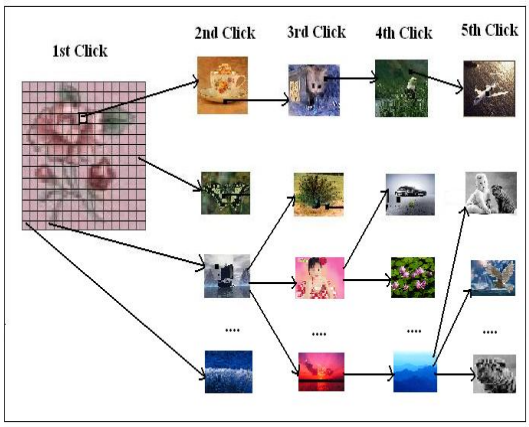

Figure 2. Example of a Click-based password scheme

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

Consider that Cued Click Points fits into an authentication model where a user has a client device (which displays a message) to access an online server (which authenticates the user). The images are stored in server-side with client communication through SSL (Secure Socket Layer)/TLS (Transport Layer Security) for establishing end-to-end secure channel for internet traffic.[14] If a user enters an incorrect click point, then the sequence of images from that point onwards will be incorrect and thus the login attempt will fail[15]. For an attacker who does not know the correct sequence of images, this cue will not be helpful. A major usability improvement over Cued Click Points is the fact that legitimate users get click point was incorrect and can immediately cancel this attempt and try again from the beginning. The visual cue does not explicitly reveal "right" or "wrong" but is evident using knowledge only the legitimate user should posses.[16] Another usability improvement is that being cued to recall one point on each of image appears easier than remembering an ordered sequence of all points on one image. Cued Click Points provides greater security and usability because the number of images increases the workload for attackers.[17

To log in, the user has to click again closely to the chosen points, in the chosen sequence. Being cued as each image users have to remember only one click-point per image that appears easier than having to remember an ordered series of clicks on one image. This system analyses is done with an image of size 100x75 pixels and tolerance squares of 19x19 pixels. The function f (username, current Image, current ToleranceSquare) that uniquely maps each tolerance square to a next-image[18]. One argument against using fewer images, and having multiple tolerance squares map to the same next-image, is that this could potentially result in misleading implicit feedback in such situations where users click on an incorrect point yet still see the correct next-image.[19] A user's initial image is selected by the system based on some user characteristic (as an argument to f above; we used username). Therefore, the negative impact would be less with Cued Click Point than with PassPoints since a one-to-one mapping between images and click-points in CCP would appear to be easier for users to manage.[20]

4 Watermarking

Data watermarking is a technique for inserting information into an image, which can be later extracted or detected for variety of purposes including identification and authentication purposes. The main difference is on intent, while the purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information. Steganography can also be combined to implement watermarking.[21]

In data watermarking, the username and password is encrypted in an image and this encrypted file is saved to upload later for verification. Before user enters the password, the username is validated by uploading the encrypted file and searched in the database.[22] If the username is valid the server will allow user to enter password otherwise an error message will be displayed. This provides more security to the user credentials before entering into the website.[23]

IV CONCLUSION

Phishing has becoming a serious of network security problem, causing financial lose of billions of dollars to both consumers and e-commerce companies. And perhaps more functionally phishing has made e-commerce distrusted and less attractive to normal consumers. This project focused on users to protect themselves again phishing attacks using Cued Click Point techniques. When the user will enter login details in website, the username is encrypted and embedded by stego-image and send to server. Server will responses as image to user, to select the password from sequences of image using cued click point approach. Hence, this approach would be deployed for website requiring a high level of security in regaining victim's confidence.

Future work should include a thorough assessment of the viability of Cued Click Point as an authentication mechanism, including a long term study of how these passwords work in practice and whether longer CCP passwords would be usable. The security of Cued Click Point also deserves closer examination, and should address how attackers might exploit the emergence of PassPoints.

REFERENCES

1. R. Anderson (Nov 1994), "Why Cryptosystems Fail," Communications of the ACM, 37(11), pp.32-40
2. Bank of America (Jan 23, 2007), "How Bank of America SiteKey Works for Online Banking Security", http://www.bankfamerica.com/privacy/siteKey/
3. Brubaker, Bill (July 14, 2007), "Bank of America Personalizes Cyber- Security", Washington Post, http://www.washingtonpost.com/wpdyn/content/article/2005/07/13/AR2005071302181.html

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

4. Krishnamoorthy P., Jayalakshmi T., "Preparation, characterization and synthesis of silver nanoparticles by using phyllanthusniruri for the antimicrobial activity and cytotoxic effects", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(11) (2012) pp.4783-4794.
5. C. Cachin, "An Information-Theoretic Model for Steganography", in *proceeding 2nd Information Hiding Workshop*, vol. 1525, pp. 306-318, 1998.
6. R. Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE pp. 1019-1022, 2001.
Madhubala V., Subhashree A.R., Shanthi B., "Serum carbohydrate deficient transferrin as a sensitive marker in diagnosing alcohol abuse: A case - Control study", Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 7(2) (2013) pp.197-200.
7. R. Dhamija and J.D. Tygar (July 2005), the battle against phishing: Dynamic Security skins. In ACM symposium on usable security and privacy (SOUP '05).
8. R. Dhamija and J.D. Tygar (May 2005), Phish and HIPs: Human interactive proofs to detect Phishing attacks. In Human Interactive Proofs: Second International Workshop-HIP.
9. Khanaa V., Thooyamani K.P., Saravanan T., "Simulation of an all optical full adder using optical switch", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6)(2013) pp.4733-4736.
10. Ford W. and Kaliski Jr., B.S. (2000) "Server-assisted generation of a strong secret from a password", WETICE'00: Proceedings of the 9th IEEE international Workshops on Enabling technologies, Washington, DC, USA: IEEE Computer Society, pp.176-180. http://www.rsa.com/rsalabs/staff/bios/bkaliski/publications/password.
11. Hoffman, Patrick (Jan 10, 2007), "RSA Catches Financial Phishing Kit", http://www.eweek.com/article2/0,1895,2082039,00.asp
12. Nagarajan C., Madheswaran M., "Stability analysis of series parallel resonant converter with fuzzy logic controller using state space techniques", Electric Power Components and Systems, ISSN : 1532-5008, 39(8) (2011) pp.780-793.
13. Jakobsson M. (2005) Modeling and Preventing Phishing attacks. In Financial Cryptography, http://www.informatics.indiana.edu/markus/papers/phishing_jakobsson.pdf
14. Jakobsson M. and Young A. (Mar 2005), Distributed Phishing attacks, Workshop on Resilient Financial Information Systems.
15. Bhat V., "A close-up on obturators using magnets: Part I - Magnets in dentistry", Journal of Indian Prosthodontist Society, ISSN : 0972-4052 , 5(3) (2005) pp.114-118.
16. Jason wells, Damien Hutchinson, Justin Pierce., (2008), "Enhanced Security for Preventing Man-in-the-Middle Attacks in Authentication, Data Entry and Transaction Verification http://igneous.scis.ecu.edu.au/proceeding/2008/asm/Hutchinson%20Enhanced%20Security.pdf
17. John Engler, Chris Karlof, Elaine Shi, Dawn Song., (2000)" Is it too late for PAKE?"
18. Kuo C. Parno B. and Perrig A. (2006) "Phool-Proof Phishing Prevention Proceedings Financial Cryptography and Data Security, http://sparrow.ece.cmu.edu/group/pub/parno_kuo_perig_phoolproof.pdf
19. Leyden J. (Aug 2005), Spear Phishers launch targeted attacks, http://www.theregeister.co.uk/2005/08/02/ibm malware report/
20. Mayer S. (June 2008), "Delayed Password Disclosure", Trustworthy Interfaces for Passwords and Personnel Information (TIPPI) Workshop
21. Wikipedia, http://wikipedia.org/wiki/Phishing.
22. http://crypto.stanfoird.edu/Spoof/Guard.
24. M.Sundararajan & R.Pugazhanthi," Human finger print recognition based biometric security using wavelet analysis", Publication of International Journal of Artificial Intelligent and Computational Research, Vol.2. No.2. pp.97-100(July-Dec 2010).
25. M.Sundararajan & E.Kanniga," Modeling and Characterization of DCO using Pass Transistor", proceeding of Springer – Lecturer Notes in Electrical Engineering-2011 Vol. 86, pp. 451-457(2011). ISSN 1876-1100.(Ref. Jor- Anne-II)
26. M.Sundararajan & C.Lakshmi, "Wavelet based finger print identification for effective biometric security", Publication of Elixir Advanced Engineering Informatics-35(2011)-pp.2830-2832.
27. M.Sundararajan, "Optical Instrument for correlative analysis of human ECG and Breathing Signal" Publications of International Journal of Biomedical Engineering and Technology- Vol. 6, No.4, pp. 350-362 (2011). ISSN 1752-6418.(Ref. Jor-Anne-I
28.. M.Sundararajan, C.Lakshmi & D.Malathi, "Performance Analysis Restoration filter for satellite Images" Publications of Research Journal of Computer Systems and Engineering-Vol.2, Issue-04- July-December-2011-pp 277-287