Countering Phishing Threats using Visual Cryptography

G. Pavithra[1], D. S. John Deva Prasanna[2]

[1, 2] School of Computing Sciences
Hindustan University
pavi.teddy24@gmail.com
johndp@hindustanuniv.ac.in

Abstract: ***Phishing is an attempt by an individual or a group to get personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. Fake websites which appear very similar to the original ones are being hosted to achieve this. In this paper we have proposed a new approach named as "Countering Phishing Threats using visual cryptography" to solve the problem of phishing. Phishers can attack the most confidential information of the user from the authorized websites. Here an image based authentication using Visual Cryptography is implemented. In Visual Cryptography (VC) an image is decomposed into shares and in order to reveal the original image appropriate number of shares should be combined. The use of visual cryptography is explored to preserve the privacy of an image captcha by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image captcha. Due to frequent change in image captcha the authenticated information like password cannot be stolen by the phisher. Once the original image captcha is revealed to the user can be used as the password. Using this cryptography methodology, we can verify its identity and proves that it is a genuine website before the end user.***

Keywords: visual cryptography, image captcha, uniform resource language, visual Cryptography Scheme.

1. Introduction

Web Security is a branch of computer security that deals specifically with Internet-based threats. These include hacking, where unauthorized users gain access to computer systems, email accounts or websites; viruses and other malicious software (malware), which can damage data or make systems vulnerable to other threats; and identity theft, where hackers steal personal details such as credit card numbers and bank account information. You can protect yourself from these threats with strong Internet security. We have just studied two important areas where security is needed: communications and e-mail. You can think of these as the soup and appetizer. Now it is time for the main course: Web security. The Web is where most of the Trudies hang out nowadays and do their dirty work. In the following sections we will look at some of the problems and issues relating to Web security. Web security can be roughly divided into three parts. First, how are objects and resources named securely? Second, how can secure, authenticated connections be established? Third, what happens when a Web site sends a client a piece of executable code? After looking at some threats, we will examine all these issues. Numerous sites have been brought down by denial-of-service attacks, in which the cracker floods the site with traffic, rendering it unable to respond to legitimate queries. Often the attack is mounted from a large number of machines that the cracker has already broken into (DDoS atacks). These attacks are so common that they do not even make the news any more, but they can cost the attacked site thousands of dollars in lost business.

1.1 Introduction to the project

Phishing attacks are a major concern for preserving Internet user's privacy. By combining social engineering and website forgery techniques, phishing attacks spoof the identity of a company (typically a bank or an auction site), to trick Internet users to reveal confidential information (e.g. login, password, credit card number).The perfect phishing attack creates a website very similar to the legitimate one by using the same logos, images, structure, etc. However, if the user examines attentively the URL displayed in the address bar of the web browser, he should notice that the URL (especially the domain name) is not the usual one. Other kinds of phishing attacks – i.e. the pharming attacks – are much more complex to detect because both the visited URL and the website are similar to the legitimate site. Pharming attacks aim to corrupt DNS information to redirect users to a fraudulent website under the control of the attacker. DNS vulnerabilities can be exploited at the client-side - by corrupting the user/company computer or the border router -, but also in the ISP network or at the server-side - by intercepting, modifying or spoofing DNS exchanges as well as using content injection code techniques. As DNS Sec protocol is not fully deployed today over the whole Internet infrastructure to provide end-to-end secured DNS exchanges, we can hardly protect the user from DNS corruptions, especially for the attacks that occur in his own network.

1.2 Motivation for the work

According to the cryptography techniques, one can create fake or phishing web pages. The different procedures can be used to make fake page for other websites like yahoo, msn, or any other sites which you want to steal the password of particular user. Password can be easily hacked by the hackers with the fake page. The users have to check it out with the original web page. This hacking method can be overcome by my project "Countering Phishing Threats Using Visual Cryptography".

2. Literature Survey

2.1 A visual cryptography coding system for jam resistant communication

A form of visual jam resistant coding is presented. Using Visual BBC, a modified form of BBC (Baird, Bahn, Collins) coding, it is shown that several images can be printed on clear plastic, such that when they are superimposed (i.e., a bitwise OR of the pixels is performed), the resulting image may look random, but the original images can still be recovered without any information about the original pictures and without any secret. BBC is a complex subject to understand, and so Visual BBC aids the teaching of how BBC coding works, by giving students a concrete, physical model. Examples are shown, illustrating that it is possible for legitimate BBC code words to actually look like recognizable images, rather than just random binary strings. This allows us to superimpose arbitrary pictures and separate them again in linear time without using any keys or channels specific to each picture. This is not possible in any other coding systems, such as error correcting codes, superimposed codes, or steganography systems. In addition, a number of analysis problems are described that can be given to students, which are motivated by the issues arising in Visual BBC, and which further increase student understanding of the system.

2.2 Visual cryptography for authentication using captcha

Authenticity of the user is the major issue in today's internet applications such as core banking. Password has been the most used authentication mechanism which is subjected to offline and online dictionary attacks. Today hacking of the databases on the internet is unavoidable. It is difficult to trust the information on the internet. To solve this problem this paper proposes a CAPTCHA based Visual Cryptography scheme to address the authentication issues. This methodology generates a unique CAPTCHA image for users which in turn is divided into two shares. One share is stored in the bank database and the other share is provided to the customer. Hash code is generated for the customer share and it is stored in the bank database. The customer has to present the share during all of his/her transactions. When the customer presents his share the hash code is generated and compared with the database value. If it matches the shares are stacked to get the original CAPTCHA image which authenticates the user.

2.3 The phishing guide understanding & preventing phishing attacks

Phishes have made use of an increasing array of delivery systems in order to fool their victims in to handing over confidential and personal information. Even after more than 10 years of phishing attacks and much publicity, phishing scams are still hugely profitable to the professionals who run them. While phishes develop ever more sophisticated attack vectors, businesses continue to flounder to protect their customers' personal data. Customers have become wary of "official" e-mail and question the integrity of the Websites they now connect to as their confidence and trust wanes .With various governments and industry groups battling their way to prevent spam, organizations can in the meantime take a proactive approach in combating the phishing threat. By understanding the tools and techniques used by these professional criminals, and analyzing flaws in their own perimeter security or applications, organizations can prevent many of the most popular and successful phishing attack vectors. This updated paper covers the technologies and security flaws phishers exploit to conduct their attacks, and provides detailed vendor-neutral advice on what organizations can do to prevent future attacks. Armed with this information, security professionals and customers can work to protect themselves against the next phishing scam to reach their inboxes.

2.4 Segment-based visual cryptography

A version of Visual Cryptography is presented which is not pixel-based but segment-based. It is used to encrypt messages consisting of symbols which can be represented by a segment display. For example, the decimal digits 0;:::; 9 can be represented by the well-known seven- segment display. The advantage of the segment-based encryption is that it may be easier to adjust the secret images and that the symbols are potentially easier to recognize for the human eye, especially in a transparency-on-screens scenario.

2.5 Protecting browsers from DNS rebinding attacks

DNS rebinding attacks subvert the same original policy of browsers and convert them into open network proxies. We survey new DNS rebinding attacks that exploit the interaction between browsers and their plug-ins, such as Flash Player and Java. These attacks can be used to circumvent firewalls and are highly cost-effective for spending spam email and defrauding pay-per-click advertisers, requiring less than $100 to temporarily hijack 100,000 IP addresses. We show that the classic defense against these attacks called "DNS pinning," is ineffective in modem browsers. The primary focus of this work, however, is the design of strong defenses against DNS rebinding attacks that protect modem browsers. We suggest easy-to-deploy patches for plug-ins that prevent large-scale exploitation, provide a defense tool, dns wall, which prevents firewall circumvention, and detail two defense options, policy based pinning and host name authorization.

3. Existing System

Logging in with username, password and secret pin number is common on the internet and passwords are widely being used by web mail providers. One of the attacks on password is Phishing. Phishing is a kind of attack in which victims are tricked by spoofed emails and fraudulent web sites into giving up personal information. The existing anti-Phishing technique, PwdHash technique is ineffective against some attack. Phishers stole the database entries and then tries hashes and after an exhaustive search they get the password. During implementation SHA-1 is more secure but slow in execution as SHA-1 includes more rounds comparatively.

Pharming attacks – a sophisticated version of phishing attacks – aim to steal users' Credentials by redirecting them to a Fraudulent Website using DNS-based Techniques.

4. Proposed System

This research attempted to provide solution to password login attacks and implemented MD5 and checked their performances. If the password is hashed with addition of salt by applying a cryptographic hash function, then Phishing attack can be removed. The salt value will prevent attackers from building a list of hash values for common passwords. Here some parameters like URL validation, domain validation through WHOIS are used to identify the Phishing site. In this paper, password hashing has been described with MD5 hashing algorithms that strengthens web password authentication. It is also shown that the attack on hashed passwords is unsuccessful as getting original password from hashed form is not an easy task due to addition of salt value. If the user is valid get a session key via mobile, through which further access can be done to provide anti Pharming technique. Pharming attacks can be prevented using the implementation of verification of Domain Name, IP Address, Who is Server, Inter Domain and Web Content. Every Website should have registered those information would be founded using Who is Server. Pharming attack is looks same as original website and obtains all the Sensitive Information's from the Legitimate User and can get money by providing those inputs in the original (Banking) website. The detecting methods are ensuring 95% accuracy in identifying Pharming Attacks.

4.1Advantages of Proposed System

If the user unfortunately login into the Phishing site an automatic alert will be displayed. Each and every time an user enter the username and password to the website an random number is sent to the users mobile phone. Even the Phishers get the secret number they can't perform any transaction without the random number.

5. System Architecture

It represents the Architecture of Countering phishing threats using visual cryptography.

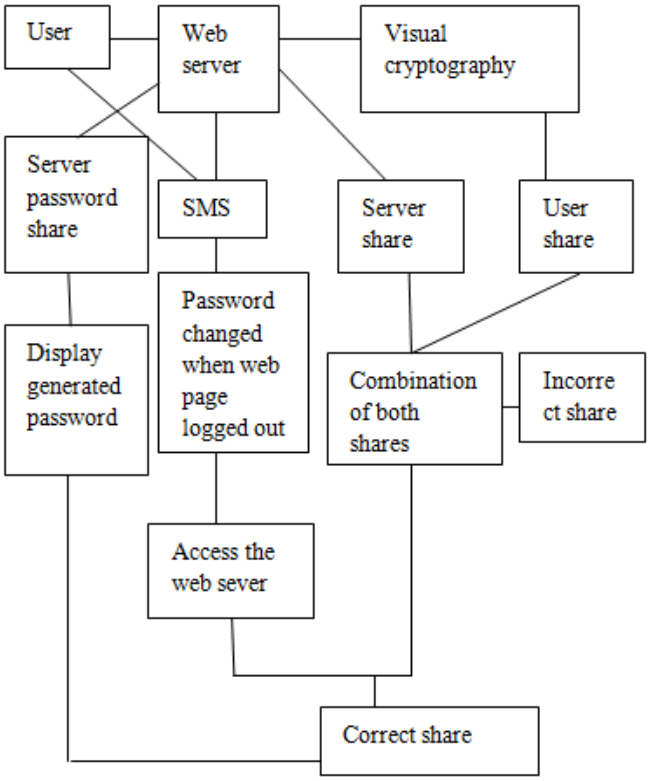

Figure 1: Architecture of Countering phishing threats using visual cryptography

5.1 Problem Definition

PwdHash technique is ineffective against some attack. Phishers stole the database entries and then tries hashes and after an exhaustive search they get the password. During implementation SHA-1 is more secure but slow in execution as SHA-1 includes more rounds comparatively. Pharming attacks – a sophisticated version of phishing attacks – aim to steal users' Credentials by redirecting them to a Fraudulent Website using DNS-based Techniques.

5.2 Overview of the Project

A text classifier, an image classifier, and an algorithm fusing the results from classifiers are introduced. An outstanding feature of this paper is the exploration of a Bayesian model to estimate the matching threshold. This is required in the classifier for determining the class of the web page and identifying whether the web page is phishing or not. In the text classifier, the naive Bayes rule is used to calculate the probability that a web page is phishing. In the image classifier, the earth mover's distance is employed to measure the visual similarity, and our Bayesian model is designed to determine the threshold. In the data fusion algorithm, the Bayes theory is used to synthesize the classification results from textual and visual content. The effectiveness of our proposed approach was examined in a large-scale dataset collected from real phishing cases. Experimental results demonstrated that the text classifier and the image classifier we designed deliver promising results, the fusion algorithm outperforms either of the individual classifiers, and our model can be adapted to different phishing cases. It consists of seven modules. They are:

- Registration: This module places a vital role in this project because this is deviated from normal registration process. Because in this module the client will register all his authentication information along with his user Name, password, gender, Mobile number, Age, DOB, Address. All the information is stored in the Main Server for Authentication.

- Server: A server is a computer program running to serve the requests of other programs, the "clients". Thus, the "server" performs some computational task on behalf of "clients". The clients either run on the same computer or connect through the network.

- Here the Server acts as the main resource for the client. Server is responsible for maintaining all the client information. Server will prevent the unwanted users entering into the network. It also verifies the access privileges of each and every user. The users have to be in their limits.

- Session Key Generation: Once the user is successfully authenticated, a session key will be generated using Secured Random Number Generation Algorithm and that will be send to the user's mobile as one time password.

- Validation of Phishing Site: The main DNS server is having all the information of Original & Phishing Web sites. Each web site has who is information along with the IP address. WHO IS, is all about the website registration, name to which the web site is registered, along with the company details. Every Web site has a IP address, which will be used for authentication. Phishing Database is always updated with the Phishing Website's details for verification.

  The DNS server will also have the complete details regarding the Domain Name & Inter domain in the web address. Each & every web site will have Domain name (.Com, .Co, .in, .Edu, .Tech, .Co, .uk, .in, Org & etc). Inter domain is all about any two domain names in the same link. Phishing Database is always updated with the Phishing Website's details for verification.

- Visual Cryptography: During Registration phase, the user is requested to browse the fingerprint image of the user. That image will be split into two shares. One share will be saved in the server and one share will be provided to the user. Once the user login into the site, the user will provide the share that they have. The server will compare it with the share saved in their database. If the shares matched, user will be allowed to do further process.

- Authentication: Each time when the user logouts from the site, a new key will be generated and send to the user mobile. When the user logs into the site next time, they need to provide one half of the session key and the server will provide the next half of the session. Once it was matched the user is allowed perform the transaction. By implementing this module, the user can identify the site is original or Phishing site.

- Transaction: The client further initializes the transaction by session login. This module provides banking functionalities to authenticated end user or client. Client can access the required functionalities from this application. Client can access balance enquiry, and also perform money transaction in a secured way from online banking in this module we have two sub modules:

- Perform transaction
- Balance Enquiry

6. Analysis Report

The level of usability is based on three factors. They are,

- Ease of identify the fake website using Anti phishing.
- Ease of security using one time password.
- Ease of logging into the website with the authenticated password.
- Based on usability survey,
  - About 20% of users – identify the fake website.
  - About 30% of users – find the ease of security.
  - About 50% of users – ease of login into the website.

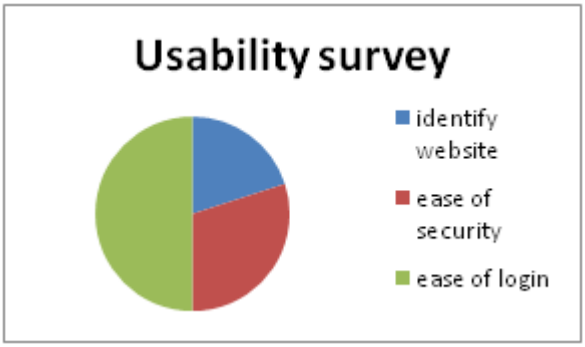

Figure 2: Usability Survey

7. Conclusion

In this proposal we compare the requested site with the WHOIS server to validate whether the site is a registered one or not. WHOIS stores entire LUI information rather than only a URL of a web site in the white-list to provide a more secure environment, especially it can efficiently defend the harming. Moreover, authentication server contains the white-list for the user. As our experiment shows, WHOIS identities a successful login process efficiently; unfortunately if the user entered into a phishing site , they can't miss use their detail because of additional authentication like token number. The warnings to the user will be more and more accurate.

8. Future Enhancement

In future, we will use a more private device (smart phone) to store white-list in a more secure environment. More experiments with larger datasets will also be preformed to

make AIWL (Automated Individual White-List) more efficient. The change rate of IP should be a big problem in AIWL, longer time-span need to be used to gather the web sites' IP and analyze.

References

[1] Ollmann G, the Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research

[2] M.Naor and A.Shamir (1994), "Visual cryptography," in Proc. EUROCRYPT, pp. 1–12

[3] A. Shamir (1979), .How to Share a Secret, Communication ACM, vol. 22, pp. 612-613.

[4] G.R. Blakley(1970), Safeguarding Cryptographic Keys,. Proceedings of AFIPS Conference, vol. 48, pp. 313-317.

[5] A.Menezes, P. Van Oorschot and S. Vanstone(1997), .Handbook of Applied Cryptography, CRC Press, Boca Raton, FL.

[6] B. Borchert(2007), Segment Based Visual Cryptography, WSI Press, Germany.

[7] W-Q Yan, D.Jin and M. S. Kanakanahalli(ISCAS-2004).Visual Cryptography for Print and Scan Applications,. IEEE Transactions, pp.572-575

[8] Sun Bin.; Wen Qiaoyan.; Liang Xiaoying.(2010); "A DNS based Anti-Phishing Approach," in Proceedings of IEEE- Second International Conference on Networks Security, Wireless Communications and Trusted Computing.

[9] Wenyin Liu, Xiaotie Deng, Guanglin Huang, and Anthony Y. Fu, "An Anti phishing Strategy Based on Visual Similarity Assessment", IEEE Internet Computing, v 10, n 2, p 58-65, March/April 2006.

[10] JungMin Kang, DoHoon Lee, "Advanced White List Approach for Preventing Access to Phishing Sites", 2007 International Conference on Convergence Information Technology, ICCIT 2007, p 491-496, 2007

Author Profile

G. Pavithra received bachelor's degree (Arunai Engineering College) in Computer Science and Engineering from Anna University, Chennai, India in 2011 and doing Master's degree in Computer Science and Engineering from Hindustan University, Chennai.