www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 293-297

e-ISSN : 2583-1062

Impact Factor : 5.725

SUBSTANTIAL DIAGNOSIS OF FRAUD INVESTIGATION USING VISUAL CRYPTOGRAPHY

Neya Sridhar[1], Mr. E. R. Ramesh[2], Ms. Sarika Jain[3], Dr. S. Geetha[4]

[1]M. Sc – CFIS, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

[2,3]Center of Excellence in Digital Forensics, Chennai 600 089, Tamilnadu, India

[4]Professor and Head, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

ABSTRACT

Phishing detection is recognized as a criminal issue of Internet security. By deploying a gateway anti-phishing in the networks, these current hardware-based approaches provide an additional layer of defense against phishing attacks. Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information etc. from unsuspecting victims for identity theft, financial gain and other fraudulent activities. The first defense should be strengthening the authentication mechanism in a web application. A simple username and password-based authentication is not sufficient for web sites providing critical financial transactions. In this paper we have proposed a new approach for phishing websites classification to solve the problem of phishing. Phishing websites comprise a variety of cues within its content-parts as well as the browser-based security indicators provided along with the website. The use of images is explored to preserve the privacy of 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. Once the original image captcha is revealed to the user it can be used as the password. Several solutions have been proposed to tackle phishing. We organize the existing literature based on detection techniques for different attack vectors (e.g., URLs, websites, emails) along with studies on user awareness. For detection techniques we examine properties of the dataset, feature extraction, detection algorithms used, and performance evaluation metrics.

1. INTRODUCTION

Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanism should also be so effective. 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. Since the design and technology of middleware have 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. phishing is a form of online identity theft that aims to steal sensitive information such as 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.

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 electronic communication".

2. LITERATURE SURVEY

Nektarios Leontiadis et.al,

Merits- We find that about one-third of all search results are one of over 7 000 infected hosts triggered to redirect to a few hundred pharmacy websites. Legitimate pharmacies and health resources have been largely crowded out by search redirection attacks and blog spam.

Demerits-Infections persist longest on websites with high Page Rank and from Edu domains. 96% of infected domains are connected through traffic redirection chains, and network analysis reveals that a few concentrated communities link many otherwise disparate pharmacies together. We calculate that the conversion rate of web searches into sales lies between 0.3% and 3% and that more illegal drugs sale is facilitated by search-redirection attacks than by email spam.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 293-297

e-ISSN : 2583-1062

Impact Factor : 5.725

Zhou Li et.al,

Merits- In this paper, using nearly 4 million malicious URL paths crawled from different attack channels; we perform a large-scale study on the topological relations among hosts in the malicious Web infrastructure. Our study reveals the existence of a set of topologically dedicated malicious hosts that play orchestrating roles in malicious activities.

Demerits- Despite the plethora of forms of attacks and the diversity of their delivery channels, in the back end, they are all orchestrated through malicious Web infrastructures, which enable miscreants to do business with each other and utilize others' resources. Identifying the linchpins of the dark infrastructures and distinguishing those valuable to the adversaries from those disposables are critical for gaining an upper hand in the battle against them.

Kyle Soska et.al,

Merits- In this paper, we take a complementary approach, and attempt to design, implement, and evaluate a novel classification system that predicts, whether a given, not yet compromised website will become malicious in the future. We adopt several techniques from data mining and machine learning which are particularly well-suited for this problem.

Demerits-A key aspect of our system is that the set of features it relies on is automatically extracted from the data it acquires; this allows us to be able to detect new attack trends relatively quickly. We evaluate our implementation on a corpus of 444,519 websites, containing a total of 4,916,203 Web Pages, and show that we manage to achieve good detection accuracy over a one-year horizon; that is, we generally manage to correctly predict that currently benign websites will become compromised within a year.

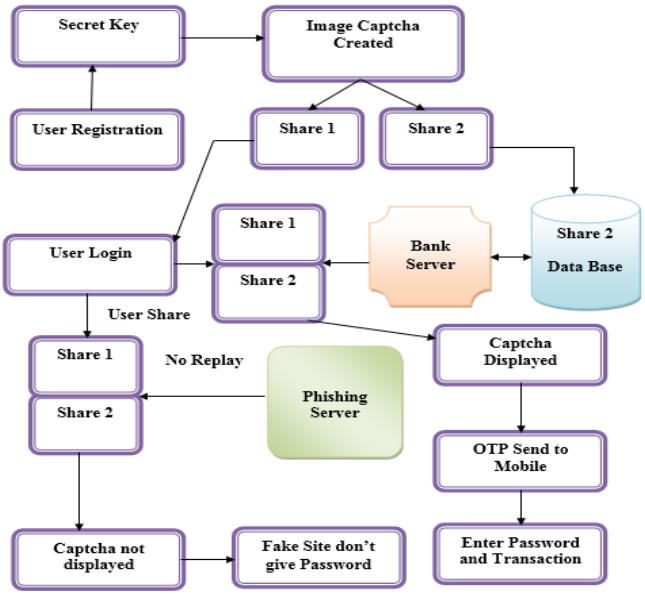
3. EXISTING SYSTEM

Password authentication is one of the most likely used authentication techniques. Secure password storage is the most difficult process. In this paper, we propose a password confirmations structure that is intended for secure password storage and could be effectively coordinated into existing authentication systems. In this project, first, we receive the plain text from the user then hashed through a cryptographic function. In the next step, hashed password is converted into a negative password. Finally, the negative password is encrypted into an Encrypted Negative Password using an encryption algorithm. Challenge-response authentication and multi-factor authentication could be employed to further improve security.

4. PROPOSING SYSTEM

The concept of image processing and improved visual cryptography is used. Image processing is a technique of processing an input image and getting the output as either an improved form of the same image and/or characteristics of the input image. In Visual Cryptography (VC) an image is decomposed into shares and to reveal the original image appropriate number of shares should be combined. 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.

5. ARCHITECTURE DIAGRAM



www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

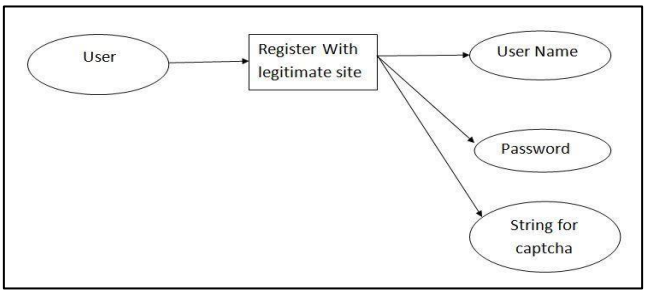
Vol. 03, Issue 04, April 2023, pp : 293-297

e-ISSN : 2583-1062

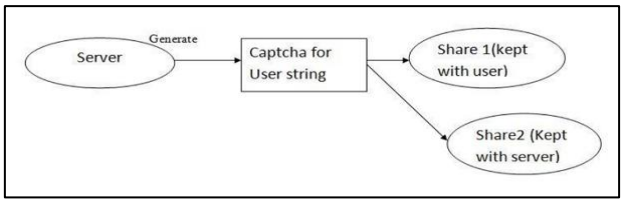
Impact Factor : 5.725

6. DATA FLOW DESIGN

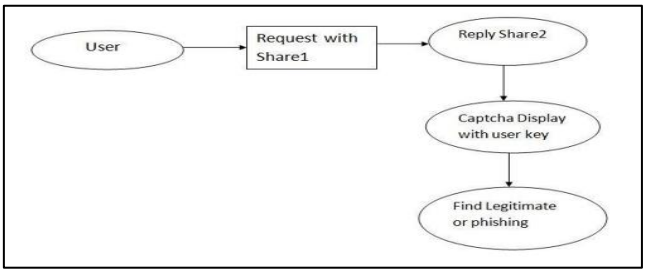
0-Level DFD



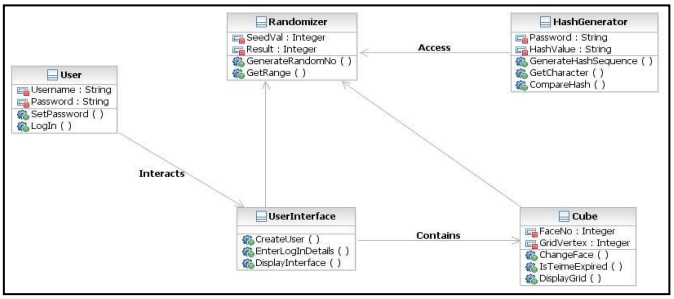
1-Level DFD



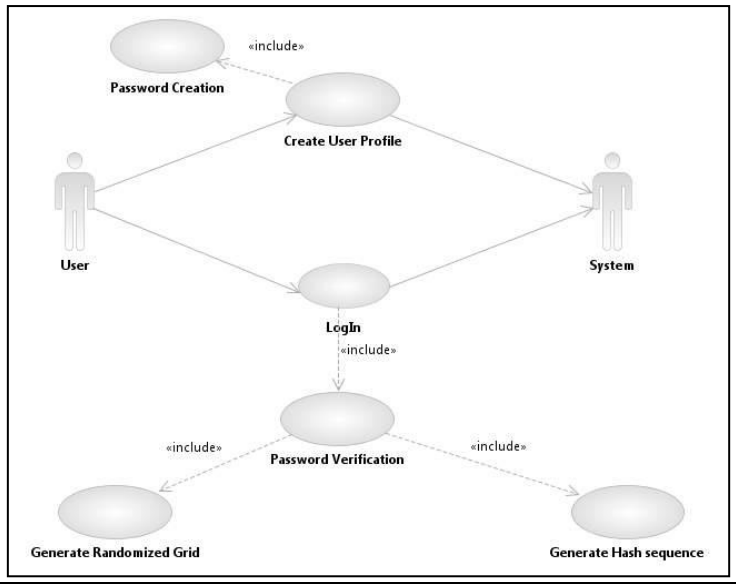
2-Level DFD



Detailed Design



Program Structural Design



www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 293-297

e-ISSN : 2583-1062

Impact Factor : 5.725

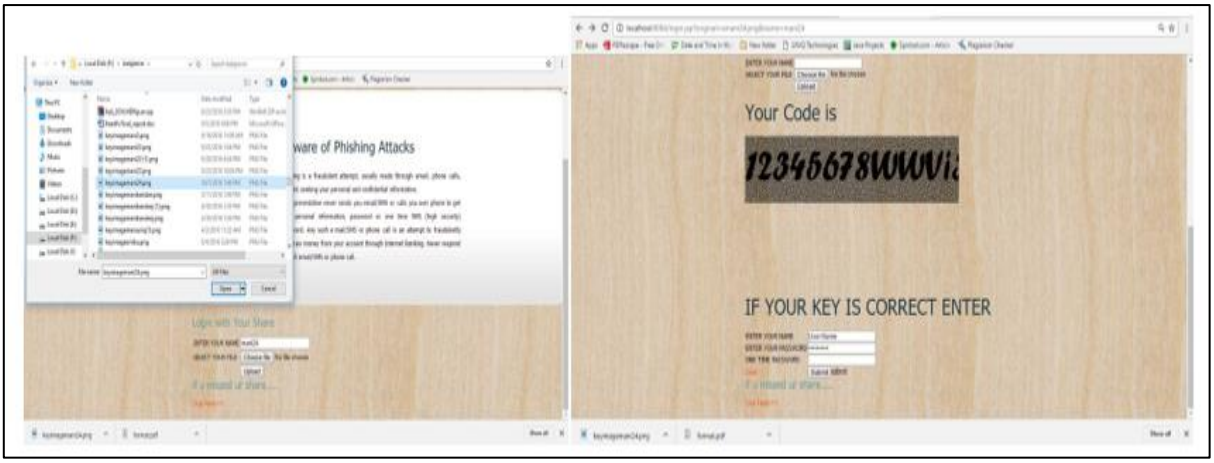
7. SCREEN SHOTS

Login page

Registration

Captcha generation

Key search



8. CONCLUSIONS

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.

9. REFERENCES

[1] N. Leontiadis, T. Moore, and N. Christin, "Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade," in Proceedings of USENIX Security 2011, San Francisco, CA, Aug. 2011.

[2] Z. Li, S. Alrwais, Y. Xie, F. Yu, and X. Wang, "Finding the linchpins of the dark web: A study on topologically dedicated hosts on malicious web infrastructures," in 34th IEEE Symposium on Security and Privacy,2013.

[3] K. Soska and N. Christin, "Automatically detecting vulnerable websites before they turn malicious," in Proceedings of the 23rd USENIX Security Symposium (USENIX Security'14), San Diego, CA, Aug. 2014, pp. 625–640.

[4] Doupe A, L. Cavedon, C. Kruegel, and G. Vigna, "Enemy of the State: A State-Aware Black-Box Vulnerability Scanner," in Proceedings of the USENIX Security Symposium, Bellevue, WA, August 2012.

[5] B. Wardman, G. Shukla, and G. Warner, "Identifying vulnerable websites aby analysis of common strings in phishing URLs," in Proceedings of the Fourth eCrime Researchers Summit. IEEE, 2009, pp. 1–13.

[6] J. P. John, F. Yu, Y. Xie, A. Krishnamurthy, and M. Abadi, "Heatseeking honeypots: Design and experience," in Proceedings of the 20th International Conference on the World Wide Web. ACM, 2011, pp. 207–216.

[7] D. Wang, S. Savage, and G. Voelker, "Cloak and dagger: Dynamics of web search cloaking," in Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM, 2011, pp. 477–490.

[8] L. Carlinet, L. M´e, H. Debar, and Y. Gourhant, "Analysis of computer infection risk factors based on customer network usage," in Conference on Emerging Security Information, Systems and Technologies. IEEE, 2008, pp. 317–325.

[9] D. Moore, C. Shannon, and J. Brown, "Code-Red: a case study on the spread and victims of an internet worm," in Proceedings of 2nd ACM/USENIX Internet Measurement Workshop, Marseille, France, Nov. 2002, pp. 273–284.

[10] Pitsillidis A, C. Kanich, G. Voelker, K. Levchenko, and S. Savage, "Taster's choice: A comparative analysis of spam feeds," in ACM SIGCOMM Conference on Internet Measurement, 2012, pp. 427–440.