Defensive Schemes of Phishing Attacks

Kusuma.N[1], Anil Subhas.V[2]
[1, 2]Department of Computer networks and security
[1]Gitam University, Hyderabad
[2]CYIENT

Abstract-*Phishing which is a kind of theft that attempting to steal sensitive information, has become a major threat to people's daily life. Some researchers proposed some methods of anti-phishing based on the characteristics of fishing behaviors. This article will firstly introduce the field of phishing and some mature method for anti-phishing. Then, it will propose an effectively phishing website detection system called IPDS to prevent phishing attacks, and finally, it will summarize this technical report and point out some directions for the future research.*

Keywords-phishing, anti-phishing, detection system

I. INTRODUCTION

Phishing is a kind of theft that attempting to steal sensitive information like user names, passwords, bank account numbers and important business information via internet.

The first phishing appeared in 1996 [1], only few people treated it seriously. Nowadays, the internet becomes an important part of our common lives. For instance, more than billions of American dollars business processes online, thus it is inevitable to attracts criminals attention. According to a survey, US commerce lose more than 2 billion American dollars every year because of phishing [2], and in 2007, the number of lost money increased to 3.2 billion American dollars [3].

This technical report will mainly focus on proposing an effectively phishing website detection system to prevent phishing attacks. Firstly, section two will introduce how does phishing works. Then section three will specify some common behaviors of phishing attacks. Then, section four will evaluate current anti-phishing solutions. Next section five will propose an effectively phishing website detection system to prevent phishing attacks. Finally, section six will give a conclusion and point out some directions for the future research.

II. HOW DOES PHISHING WORK?

Phishing is set up to look as legitimate and as genuine as possible by creating an email and web page that is almost identical to an official email and website of a trusted organisation, or by injecting untrusted data within an existing authentic website. The email sent by the phishers will include a link to what appears to be an “official” website, which is actually a fake site operated by the attacker. Once you have visited this website, any information you enter on the web page will be collected by the phisher and may be used fraudulently for whatever purpose the phisher has in mind.

From beginning to end, the process involves[4]:

Planning – A phisher decides which business to target and determines how to obtain email addresses for the customers of that business. They often use the same mass□mailing and address collection techniques as spammers.

Setup – Once they know which business to spoof and who their victims are, the phisher creates methods for delivering the message and collecting the data. Most often, this involves email addresses and a web page.

Attack – This is the step people are most familiar with □ the phisher sends a phony message that appears to be from a reputable source.

Collection – The phisher records the information victims enter into web pages or popup windows.

Identity Theft and Fraud – The phisher uses the information they've gathered to make illegal purchases, or otherwise commit fraud.

If a phisher wishes to coordinate other attacks, he will evaluate the successes and failures of the completed scam and begin the cycle again. Phishing scams often take advantage of software and security weaknesses on both the client and server sides, but even the most high□ tech phishing attacks work like old□fashioned con jobs, in which a hustler convinces his mark that he’s reliable and trustworthy.

III. OVERVIEW OF PHISHING ATTACKS

Phishing websites commonly disguised as the real and credible web sites to trick users by e-mail or instant messaging [5,6]. Additionally, users may also be deceived by downloading and installing some phishing software unconsciously thus allowing victims to control users' computer and steal the private information.

Phishing usually use four kinds of ways to cheat users: URL misspellings, URL misunderstanding, voice phishing and IM phishing. Voice phishing uses phone calls to cheat users and IM phishing uses instant messaging tools such as MSN to cheat users, rather than using websites. This technical report will focus on preventing the phishing attacks by websites.

IV. EVALUATION OF ANTI-PHISHING SOLUTIONS

This section will firstly introduce a famous theoretical guideline for anti-phishing solutions called the Rusty's rule, then, list three major anti-phishing technologies, and finally, evaluate the current anti-phishing researches.

A. Theoretical Guideline

There is a famous rule for advising the anti-phishing solutions called the Rusty's rule which can be summed up in three points [7].

Point 1, phishing attackers could simulate anything they can see. With the development of technical tools, creating websites is easier as well as simulating websites. For phishing attackers, it is easy to simulate an official website to trick users once they have been seen.

Point 2, there is no secret for phishing attackers such as users' usernames or passwords. Currently, the majority of password-based systems rely on users who provide some secret information to protect users' account security. However, this kind of solution is not safe enough as a result of that users can be easy tricked by phishing attackers that leaking their secret information.

Point 3, any anti-phishing solutions are only as good as the beginning. The majority of anti-phishing solutions are too complex that make users confused. For instance, if an account recovery solution needs users to provide some sensitive and personal information. It is easy for attackers creating a faked account recovery page to steal such personal information like usernames and passwords.

B. Anti-Phishing Technologies

Based on the Rusty's rule, by studying he behaviors of phishing attacks, there are mainly three anti-phishing technologies which are server-based anti-phishing technologies, browser-based anti-phishing technologies and third-party-based anti-phishing technologies.

Server-based anti-phishing technologies refer to use servers to prevent web phishing through certification, such as electronic certificates and dynamic security skin [8].

Browser-based anti-phishing technologies aim to protect users from phishing attacks by simply embedding browser plug-ins [9,10]. For instance, designers add security toolbars into the web browsers, which could show some important security information that helps users to identify phishing attacks. However, these measures need to be well supported by the Third -Party, for example, providing a blacklist of phishing websites.

Third-party-based anti-phishing technologies refer to discover and share information about phishing sites, including e-mail detection [11], network behavior detection [12], personal information protection [13], web anomaly detection [14], real-time blacklists, and the similarity test page [15, 16].

C. Critical Evaluation of current anti-phishing researches

Currently, the anti-phishing researches mainly focus on the website anomaly detection, network behavior detection and visual-based phishing website detection.

Korea researchers Jin and Yoon proposed a method of detection based on the website anomaly [17]. This method mainly based on the DOM structure of website, uses SVM (Support Vector Machine) to detect phishing website. However, this method could not deal with the images of websites; therefore, reduce the accuracy of the method.

Madhusudhanan proposed a method to detect phishing websites by simulating the behaviors of users [18], but it could not deal with the bridge and website robot attacks.

Visual-based phishing website detection could be divided into HTML-based and Image-based matching.

Owing to the flexibility of the HTML language, the dynamic and the variety of webpage elements, counterfeiters can easily make a structure which seems as the same but completely different HTML pages, leading to the complete failure of HTML matching. Image-based matching, which aims

at detecting the similarity of web, is based on the principles of human vision, thus, it is an efficient and universal measurement in detection [19].

Cordero proposed a website image detection algorithm by applying SVM, but this method can only be used for inspection in certain website, embodying complicated mathematical characteristics as well.

A.Y.Fu raised the idea of distance matching algorithm based on a pixel-based and location of the EMD [20]. In terms of the experimental results, the effects of distance matching algorithm are significantly better than that of HTML content-based inspection. Nevertheless this algorithm still has its weakness in analyzing the relationship in location between different parts of websites, only concerning colours and distribution characteristics in page images.

According to Goesta's visual principles, the relative positions dominate in human vision, therefore, this algorithm might cause failures in detecting similarity in pages resulting from no consideration for the factor of relative positions.

V. PHISHING WEBSITES DETECTION SYSTEM: IDPS

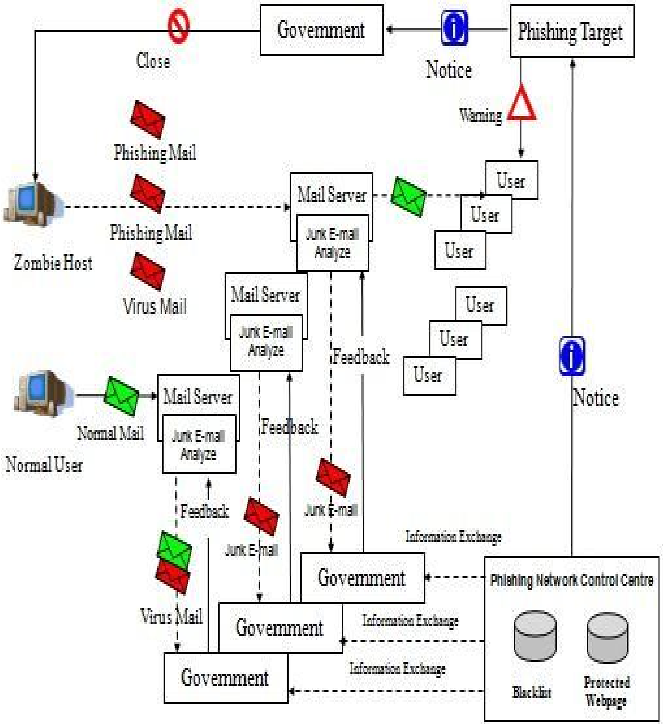
This section will propose an effectively phishing website detection system IDPS to prevent phishing attacks. Firstly, it will give a framework of phishing website detection system. Then, it will detailed explain each component of this system, which is the Junk E -mail analyzer, the node of phishing websites analysis and the phishing network control centre. Finally, it will evaluate this detection system.

A. Overall Architecture of IDPS

By reviewing the major anti-phishing technologies, the phishing websites could easily bypass the servers, and any anti-phishing technologies need to be well supported by third-party, for example, providing a blacklist of phishing websites. Therefore, the detection of phishing websites is the most important method for preventing phishing attacks.

However, considering the complexity of phishing attacks, only a single method of detecting the phishing behaviors is hard to achieve the reality goals. Therefore, it is necessary to build a systematical framework to detect the phishing websites detection.

This article proposes a framework of phishing website detection system. As the figure 1 shows, the system defines e-mail as a starting point, since E-mail is the main means of phishing by releasing deceivable pages, through mail server, the node of phishing analysis, and phishing network control centre, which is made up of a three -level preventive measures to detect and discover any phishing websites. At the same time, the system issues a warning to phishing targets such as bank, and reminds the majority of users of caution or alerts the Police Authority to prohibit phishing sites as soon as possible. Additionally, the whole system could collect and provide strong and relevant evidences for prosecuting responsible persons for creating phishing sites in legal basis. General speaking, the detecting system consists of three key elements: the Junk E-mail analyzer, the node of phishing websites analysis, as well as the phishing network control centre.



B. Junk E-mail Analyzer

Junk E-mail analyzer, located in various servers of e-mail service provider, currently has become an essential function of junk mail filtering in mail service. In order to improve the performance of collecting and filtering suspicious mails in short time, relevant phishing detection module is added into the system to enhance the process of analyzing.

C. Node of Phishing Websites Analysis

The node of phishing websites analysis could either situate in mail servers or be provided by third party. The node could obtain suspicious websites among the collection of distrustful phishing mails which are provided by the spam analyzer. Moreover, further preliminary methods such as real-time blacklists, URL and web pages detection to evaluate whether the site is phishing one or not. If the result is referring to phishing sites, an immediate notification will deliver to mail servers, while the testing result will also be sent to the phishing control centre. Otherwise, any relevant information will also be sent to control centre for further testing to avoid any uncertainty.

D. Phishing Network Control Centre

The phishing control centre has multiple responsibilities to anti- phishing activities. On the one hand, the centre focuses on maintaining the blacklist of phishing sites and protection of web database, on the other hand, it also responsible for interacting with some target phishing websites such as bank, for collecting relevant evidence and for completing the judgment and detection of phishing sites as well. Therefore the phishing control centre should qualify a distributed architecture to tackle enormous amount of tasks.

E. Evaluation

To sum up, the whole system could promptly detect phishing mails distribution and take appropriate action to forbid harms. In addition, the system could protect crucial websites such as a bank login page, through timely judgment of phishing website. The most importantly, the immediate notification to the security authority and operators against distrustful sites could safeguard the majority interests, and to help victims to recover damages since the system will collect criminal evidence of phishing websites to a great extent, which will provide an influential evidence of the law enforcement agency for detection, justice and sentence in the future

VI. CONCLUSION

Based on the understanding the behaviors of phishing attacks and evaluating the current technologies of anti-phishing solutions, this technical report proposes an effectively phishing website detection system to prevent phishing attacks which including three key components, the Junk E-mail analyzer, the node of phishing websites analysis, and the phishing network control centre.

Additionally, as the key technical of the detection system is the method of detecting phishing website, it is importantly and worthily for researchers to keep studying deeply about the method of how to divide up the image of website, how to extraction the attributes of image and how to calculate the distance of each attribute in the future.

REFERENCES

[1] M. Chandrasekaran, R. Chinchani, S. Upadhyaya, “PHONEY: Mimicking User Response to Detect Phishing Attacks,” in proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks table of contents, Washington. DC, USA, IEEE Computer Society, pp.668-672, 2006.

[2] Kerstein, Paul, “How Can We Stop Phishing and Pharming Scams?” CSO, July 19th, 2005.

[3] https://www.globalsign.com/en/resources/white-paper-phishing-attacks.pdf

[4] McCall. Tom, “Gartner Survey Shows Phishing Attacks Escalated in 2007: More than $3 Billion Lost to These Attacks,” December 17th, 2007.

[5] Duerst M, Suignard M., RFC 3987 Internationalized Resource Identifiers(IRIS)[S].The Internet Society, 2005.

[6] Berners-Lee T, Fielding R, Masinter L., RFC 3986 Uniform Resource Identifier(URI):Generic Syntax[s].The Internet Society, 2005.

[7] Dhamija, R., Tygar, J., “The battle against phishing: Dynamic security skins”, in proceedings of the Symposium on Usable Privacy and Security, July, 2005.

[8] Rachna Dhamija, J.D.Tygar, “The battle against phishing: Dynamic Security Skins,” in proceedings of the 2005 symposium on Usable privacy and security table of contents, ACM International Conference Proceeding Series, Pittsburgh, Pennsylvania, pp.77-88, 2005.

[9] M. Wu, Robert C. Miller and Simson L. Garfinke, “Do security toolbars actually prevent phishing attacks?” in proceedings of the SIGCHI conference on Human Factors in computing systems, Conference on Human Factors in Computing Systems, pp.601-610, 2006. ISBN: 1-59593-372-7.

[10] N. Chou, R. Ledesma, Y. Teraguchi, D. Boneh, and J. Mitchell, “Client-side defense against web-based identity theft,” in proceeding of 11th Network and Distributed System Security Symposium (NDSS), 2004.

[11] Inomata.A, Rahman.M, Okamoto.T, Okamoto.E, “A novel mail filtering method against phishing,” Communications, Computers and signal Processing, PACRIM, pp.221-224, 2005.

[12] M. Chandrasekaran, R. Chinchani, S. Upadhyaya, “PHONEY: Mimicking User Response to Detect Phishing Attacks,” in proceedings of the 2006 International Symposium on World of Wireless, Mobile and

Multimedia Networks table of contents, Washington. DC, USA, IEEE Computer Society, pp.668-672, 2006.

[13] D. Choi, S. Jin, H. Yoon, "A method for preventing the leakage of the personal information on the Internet," in proceedings of the 8th International Conference, Advanced Communication Technology, vol.2, pp.20-22, 2006.

[14] Thomas Raffetseder, Engin Kirda ,Christopher Kruegel, "Building Anti-Phishing Browser Plug-Ins: An Experience Report", in proceedings of the 3rd International Workshop on Software Engineering for Secure Systems, IEEE Computer Society, pp.6, 2007. ISBN:0-7695-2952-6

[15] Anthony Y. Fu, L.W., Xiaotie Deng, "Detecting phishing web pages with visual similarity assessment based on earth mover's distance (EMD)," IEEE Transactions on Dependable and Secure Computing, IEEE Computer Society Press, vol.3, no.4, pp.301-311, 2006.

[16] W.Liu, G.H, X.Liu, M.Zhang, X.Deng, "Phishing web paged etection," in proceeding of 8th interconf, documents analysis and recognition, pp.560-564, 2005.

[17] Daeseon Choi, Seunghun Jin, Hyunsoo Yoon, "A method for preventing the leakage of the personal information on the Internet", in proceedings of the 8th International Conference, Advanced Communication Technology, vol.2, pp.20-22, 2006.

[18] Madhusudhanan Chandrasekaran, Ramkumar Chinchani, Shambhu Upadhyaya, "PHONEY: Mimicking User Response to Detect Phishing Attacks. International Workshop on Wireless Mobile Multimedia archive", in proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks table of contents, Washington, DC, USA: IEEE Computer Society, pp.668-672, 2006.

[19] Anthony Y. Fu, L.W., Xiaotie Deng, "Detecting phishing web pages with visual similarity assessment based on earth mover's distance (EMD)", IEEE Transactions on Dependable and Secure Computing, IEEE Computer Society Press, vol.3 No.4, pp.301-311, 2006.

[20] Nesbitt, K.V, Friedrich.C, "Applying Gestalt principles to animated visualizations of network data", Information Visualization, 6th International Conference, pp.737-743, 2002.