중소기업융합학회 논문지 제3권 제2호 pp. 33-39, 2013

피싱/파밍 예방을 위한 인지기반 접근 방법

홍성혁*
백석대학교, 정보통신학부

Cognitive Approach to Anti-Phishing and Anti-Pharming: Survey

Sunghyuck Hong*
Baekseok University, Division of Information and Communication

요 약 현대에는 피싱 공격을 방지하는 여러 방법들이 연구 되고 있다. 이들 중에서는 작업관리창이나 브라우저의 주소창에서 피싱 사이트를 구별해 주는 프로그램들이 있다. 그러나 이런 프로그램들은 해당 사이트의 도메인이나 IP주소로 피싱 여부를 판단한다. 이 방법으로는 DNS 파밍 같은 공격은 방어할 수 있지만 숨겨진 공격(예를 들어 HTML 코드를 변경하는 기법)에는 매우 취약하다. 이 논문에서는 프로그램이 IP 나 사이트의 도메인을 분석하여 피싱 및 파밍 여부를 판단하는 기존의 방식이 아닌 플러그인과 서버 사이에서 HTML 코드의 변경 유무를 파악하고 피싱 여부를 팝업이나 플래시 등으로 위조하기 어려운 시스템 트레이와 풍선도움말을 사용하여 접속 사이트와 시스템 트레이의 그림을 사용자가 비교함으로서 직접 피싱 및 파밍 여부를 쉽게 분별할 수 있도록 하는 이미지 비교를 통한 인지 기반의 접근 방법을 제시한다.

Abstract Recently, lots of anti-phishing schemes have been developed. Several products identify phishing sites and show the results on the address bar of the internet browser. However, they determine only by domain names or IP addresses. Although this kind of method is effective against recent DNS Pharming attacks, there is still a possibility that hidden attacks which modifies HTML codes could incapacitate those anti-phishing programs. In this paper, the cognitive approach which compares images to decide phishing or Pharming is presented by using system tray and balloon tips that are hard to fake with pop-ups or flash in order for users to compare pictures from connecting sites and system tray. It differs from an old method that a program analyzes IP or domains to judge if it is phishing or Pharming. Therefore, proposed method effective cognitive approach against phishing and Pharming attacks.

Key Words : Phishing, Pharming, Hidden Attack, Graphical substitution, Cognitive approach

1. Introduction

Phishing means an individual's personal information Private data and Fishing in the sense of the compound. Phishing is using e-mail or IM reliable information of the person or company pretending sent by the user's confidential information such as passwords or credit card information illegally requiring you want to take a kind of social engineering. Phishing is a report of the accident gradually increases, studies are underway want to avoid phishing [1,2].

Such attention to the user to a phishing attack

접수일 : 2013년 9월 16일 수정일 : 2013년 9월 24일 게재확정일 : 2013년 10월 7일
*교신저자 : 홍성혁(shong@bu.ac.kr)

surface can be prevented to some extent. However, the script by using the browser's address bar and status bar cleverly covered pop-up window or the browser address bar and toolbar of the pop-up function can be deleted using the features placed at the top of your browser window toolbar to show the same picture, image rotation (Graphical Substitution) techniques are difficult to defend. The DNS Pharming (DNS Pharming), as was lawfully in possession of the DNS name of your domain, or cheated to rob the real site by mistake while persuading users how to use the site to officially operate the domain itself in the middle of oncoming seized in which case the user may enter the exact URL to be taken to a fake site [11]. In this case, the fact that the user is being attacked by damage to vulnerable groups can not even easy to understand [3].

2. Background

2.1 Phishing attack

Methods of phishing attacks E-mail phishing attacks, Pharming attacks, separated by a hidden attacks.

2.1.1 E-Mail phishing attack

Phishing 1996 American Online (AOL) Messenger of hackers using an e-mail to a user and sending operation was derived from the hacking techniques. The hackers sent their AOL e-mail is sent to e-mail users have reported cheating as users' account information.

Reason why we can not prevent such a phishing attack is a Web browser or e-mail the address bar and the link connection management program because they have weaknesses in [7]. When attacked phishing link and the address bar of the Web browser 's URL address spoofing is very similar to the actual institution and receives mail and the general public because it shows the truth of this web site, it is difficult to determine directly. In addition, information is mapped to the URL of your mouse over the image to put them on the bottom of your web browser when a malicious link that shows the link information is not a normal link so you can easily show it to be in [8,9].

2.1.2 URL Spoofing attack and IP access attack

URL addresses listed on the Internet browser address spoofing trick visit a particular site by the official site as one of the tampering. Traditionally,% 01 and% 00 in the browser does not recognize the characters as part of the URL used was similar to the normal use of the site or log in using a web browser was exploited by the way. Connected to the wrong address, even though the user to know the exact address of the site that can be mistaken as, for example, HTTP :/ / mybank.com: ebanking@ evilsite.com / phishing / is such a thing as a evilsite.com [4].

URL of the domain name by using an IP address instead of a domain name, create a content filtering to avoid confusing or as a way to disguise the destination IP address in decimal, Hex, Oct, such as a variety of shows.

2.1.3 Pharming attack

Techniques to deceive URL or DNS address of the proxy server instead of directly or indirectly modulate the Farmington phishing attacks than the user's point of view and can be more easily into. Way of farming that can be used as a modulation of the DNS address or addresses of the client to change the DNS server settings, use a proxy server, and the client host file changes, etc. There are many ways to DNS Cache Poisoning [5,6]. Phishing attacks are similar to the name of an existing domain address, or via normal redirected to the site, such as a page, using sophisticated forging fake phishing sites, but the user is guided to carefully look at what can be a phishing site was part of. Thereby changing the DNS address, but this judgment is more difficult when the user believes there is a high possibility that access.

2.1.4 Hidden Attack

The most commonly used hidden attack with a hidden frame and image replacement method Overriding Page Content [2].

Hidden behind the frame attack, attack most commonly used method is based on the frame of the attack. Figure 1 is defined by two frames show that. The first frame is a normal URL information is included, while the second frame is a hidden frame, so as to be a phishing page. Hidden frame skip to the phishing links. These attacks (Ajax captured using a script, etc.) may be leaking personal information through.

Overriding Page Content is the preferred method for inserting the content in a manner that a false real web page into the web page display on a hidden way [2]. DHTML function (DIV) using spoofed pages, insert pages are the most commonly used in the attack. This is on top of a web page, an attacker exploits the real one, including the complete page can be created. How to replace the image in the browser's address bar and get rid of the toolbar to display the image of the same shape by the bottom left of the browser to display or correct URL (Padlock Zone) HTTPS encrypted communication from the HTTP traffic look like a fool even to convert images to the user. IE 7 Starting with this technique is to force a URL to display a pop-up function, but is recognized by the Internet Explorer 7 or less using a version of the user is easily vulnerable to phishing attacks.

2.2 anti-phishing programs at home and abroad

To avoid phishing attacks, many for the current anti-phishing programs. To report a phishing site or create a blacklist of research and access to the site and check the server using SSL communication, how to use a fishing program in the opinions of users to distinguish phishing sites, social engineering, how the creation of the site how to use the information connected to the actual name of the site show that significant methods.

2.2.1 the browser's built-in phishing filter

Microsoft's Internet Explorer 7 and Firefox 3 recently came out with what is a relatively basic anti-phishing filter. The browser 's built-in browser anti-phishing filter for each company to produce a user is looking for phishing sites and phishing sites reported by creating a blacklist of phishing tactics to avoid.

2.2.2 NetCraft Toolbar

Any user connected to the server during the hosting of the registration date and the connection between the country and the Toolbar users of the site to determine the amount of the toolbar to distinguish the type of phishing program. Typical phishing sites are available for a short time, the generated stored in the browser, but the list of trusted sites in the DNS Pharming sites attacked if the program shows the problem that I trusted sites [10].

2.2.3 Trust Bar

For want to go to the site to access sites using SSL certificates with or without the logo and show the toolbar. Most of the sites are authenticated using SSL to deliver critical information to users to use SSL, but do not use a phishing site that is using SSL program. [10]. Toolbar format on how to replace the image of the program vulnerable. In addition, a small proportion compared to the entire browser toolbar icon, the user will not normally pay much attention to it if there is no information about the site as a phishing site, which also partly because of the toolbar to clear the mistake probability is high [10]. In addition, the newly created user does not have information on phishing sites are exposed to damage from fishing out the existing problems in the best anti-phishing program within the HTML code lacks an analysis of the attack code [1]. As the latest HTML technology advancement through hidden attacks can intercept your information.

3. Proposed Anti-Phishing method

Phishing sites to pop the top sites phishing sites ttuiwoomyeonseo covered with normal site again hidden away by the anti-phishing attacks can fool the program. If the URL is the same as that of farming such confusion to give users to easily [4]. In addition, the image displaying the address bar how to replace the address bar and the tool as a way to forge Management window, the user will not be easy to distinguish. HTML code HTML code tonghayeoseo hash result there has been a change in comparison to the hidden surveillance and DNS Pharming attacks and DNS spoofing attacks prevented. In addition, the communication process with the server is overloaded because it may hash the data using a symmetric encryption key to the load is prevented. After you install the plug-in to connect to the server using the URL Farmington vulnerable to DNS the IP of the server where the plug-in connection to the communication. If you want to connect to plug-in server IP has been changed within the HTML code in the server side plug-in or plug-in to call a function of the specific values of variables that can put the plug in the plug threads functions must be securely deliver IP. And the first installation of this program is assumed to be safe. If this assumption is not assuming any programs that are deployed over the Internet, because it can not be safe. Through the deployment of a secure certificate how to verify the signature was applied.

3.1 Plug-inID and Plug-inKey exchange

The plug-in is deployed in the Internet environment to guarantee the reliability of the code signing certificate has been through. To install the plug-in, without the user requesting the plug- in and plug-in, the server codebase to download the installation file will receive a certificate to verify the signature through giving is to ask users to install. However, the process of installing the first plug-in receives from phishing and Pharming attacks are dangerous to both the user and the server are correct. For this reason, the first plug-in installation process, such as the user's certificate to authenticate the user through the server at the same time on the server can authenticate the user in the process is needed.

3.2 User and server communication process

After installation, the first plug-in to connect to the server when the user performs a set of protocols. Log-in page that contains the HTML code from the server, and the server is sent SessionID with the HTML code. HTML code is received, the SessionID is a plug-in to call the user's browser. Plug-in from the server, the image shown on the balloon passed safely under it to show on the balloon in the system tray, HTML code to the browser plug- in function is called to take the name of the image shown on the browser, the login box on the server side request is displayed.

3.2.1 Web page request

Users want to connect to the server side, the server can request the HTML code to provide users with the HTML code that generates a SessionID. The resulting HTML code, the hash value of the SessionID and stored in a database on the server, and SessionID transmits the HTML code to the user. SessionID cookies, or transmitted through the HTTP GET method. HTML code, the hash value transmitted by the user to ensure the integrity of the HTML code used. Figure 2 shows the HTML code of the exchange process and shows the session ID.

3.2.2 Plug-in call and data transfer

HTML code is received from the server and the browser of the contents within the code to execute in sequence. <OBJECT> While running the code and call the plug-in through <EMBED> tag.

3.2.3 Image transfer

PID server plug-in in the database as the index C is decoded to find the key PK. Decrypting the session key

obtained as a result of two out, SID is an index into the database to the user in HTML page sent out the obtained hash value. Server, a message authentication code transmitted from the browser to the data that they have made the comparison with the message authentication code passed from any user to the server confirms whether the received data securely. If this process does not match, a message authentication code from the user, so the user is attacked and warn the image showing the Plug-in is transmitted. Match, the message authentication code, select any of the images and HTML files in the HC and the session key hash value to the hash of the data SK_E change the file name. After which the browser to send a response to a request for HTTP Request to set the image processes. HTML file name of the session key and the hash value of the code because the HTTP Request to change the browser makes a request through the attacker knows the name of a file, and at the same time in a session, the user and the server can be used in order to create a unique file name is. Users to send images to a server, then you have to change the name of the image sent from the server to the browser that the image and the hash value of the HTML code that is shared by the server and plug the plug-in sends the encrypted session key. Plug-in HTML using the session key and the image data is decoded by the hash code. HTML plug-in has a first hash value received from the server compares the hash value over HTML received from the server does not exist in the output image of the balloon does not match the hash result is the error message that the plug- in output to the balloon.

3.2.4 Image output on web browser

<EMBED> <OBJECT> Plug-in or ID tags in order to give a call. Through the ID assigned to the ID of the HTML code in the plug-in recognizes the mutual communication. Plug-in IDL (interface definition language) through a JavaScript call to the specified function can be obtained. When you call a function via javascript plug-in that has a function in the HTML code and returns the result of a session key to the hash. <IMG SRC ='ObjectID.ImageName()'.bmp> such as DOM (Document Object Model) to execute the functions of the plug-in method. This function is called by the HTML document itself and returns the hash value of the session key. The results returned by the name of the image through a request to the HTTP request, the server has passed to the plug-in to preview the HTML code and the name of the image hash of the session key has been left as a result of conversion, because it is possible to show the image. Phishing sites shown in the figure balloons to show the same picture, so users can easily phishing / Pharming will be able to determine whether or not.

3.3 Compare images

Users can provide the plug-in icon in the task bar balloons and images in your web browser to be able to distinguish compared to the phishing site. Phishing sites, phishing warning message will appear if the browser or the image is different and looks at the balloon. Balloon Help feature of the taskbar allows you to phishing sites, malicious Java code, etc. It can not be forged. In addition, the balloon that appears over the icon, the icon indicating the position of the shape of the balloon because your not a fake as can be known.

Table 1. Analysis in performance of Anti-Phishing program

	Characteristic	URL Spoofing	Access on IP	DNS Pharming	Hidden Attack
Browser filter	Blacklist	○	×	×	×
NetCraft Toolbar	Check on server's information	○	○	○	×
TrustBar	SSL Access& confirmation	○	×	○	×

4. Security Analysis

4.1 DNS Pharming analysis

By Pharming phishing sites when a user is connected to the same URL, so you do not suspect is a phishing site. The proposed technique is due to the use of plug-in plug-in to request a unique CLSID command in the HTML code must be able to invoke the plug. When another program calls CLSID Plug-in installed because it is not installed, the user will see the asking. Install the plug-in plug-ins when asked by a certificate signed by an authorized signatory to distinguish, so that if you can avoid the installation of the wrong plug. In this way an attacker would need to call in order to avoid the normal plug. Plug-in plug-in is invoked, the key exchange and the exchange of images stored by the plug- in to connect to the top of the site's IP. Plug-in connection confirmation request to the server, the user's IP check before invoking the plug-in to the user whether the HTML code can be captured. In the process, the server passes the HTML code to the user did not identify the user transmits the image to inform phishing. In addition, the plug-in phishing and Pharming sites to print the picture, even though the normal HTTP Request to request the picture in the browser 's address is a relative address instead of absolute addresses, so the image can not be displayed. In order to display an image modifies the HTML code does not match the hash result is a phishing warning plug receive a pass image. Shows a Pharming attack by DNS. Login box next to the name of the picture shown in the image hash as a result of a request by a relative address, the image of an attacker's server, so there is no file. Therefore, the image is not visible, even though the call plug is different from the hash result of the HTML code and the HTML code of the phishing warning hash result is equal to the normal picture shows the plug, but no attack was made to modify the code without the user the web as more than a browser to view the pictures confirms that phishing sites are connected.

4.2 hidden attack prevention

The proposed method is through a hash of HTML code to ensure the integrity of the HTML code. Overriding Page Content techniques, such as on a normal server-generated HTML code for the attacker to learn information you need to add code so that it is necessary to change the code. Altered code is transmitted to the user's browser plug-in is invoked, the plug-in is a result of hashing the changed HTML code to the server and the server transfers the HTML code received from the user, the hash result with the hash stored in the server by comparing the results of the HTML code, the user HTML code is changed to recognize and sent to alert the user to transmit images. In the process used to change the codes hidden attacks can be prevented. Further, the changed name of the image file created in HTML in a Web browser to display a normal image can not be performed.

4.3 Comparison with commercial programs

In this paper, we use a plug- in to change the HTML code used to analyze the hidden primary purpose is to prevent attacks. Passed between the server and the client through the HTML code by comparing the hash result hidden attacks can be captured. Current commercial programs through a comparison of the domain name and IP to prevent phishing and Pharming users or businesses phishing / Pharming site to find a way to save the black list but this Plug-in is a web browser to request the presence of the image the HTML code for comparison with the site and the user via the DNS spoofing, can be distinguished and Pharming. In addition, the image of the toolbar type of program substitution vulnerable to forge a difficult task because the images replace the management of the tray icon and balloon help line was used. However, the server calls the plug-in, this plug-in is the ability to communicate directly with the main feature and is blacklisted by the way is not used to distinguish phishing. Table 1 in Chapter 2.2 of the commercial plug-in anti-phishing attack prevention program and a comparison of this table is [12].

5. Conclusion

Hidden phishing and Pharming attacks, and attacks such as the attack is difficult to distinguish the user has to be himself. In the case of a hidden attack is enough for daily use, allowing modulation of the site to ensure the integrity of the HTML code is important. Current commercial anti-phishing solutions such as DNS spoofing, and DNS Pharming attacks, but can defend Overriding Page Content through code changes, such as user information, there are good enough to prevent the interception of a technique. The proposed anti-phishing plug-in allows a user to model the perception of phishing and at the same time able to monitor changes in the HTML code hidden by Pharming attack, and to prevent the same time DNS DNS spoofing attack can be prevented. Now and XPCOM, such as ActiveX or plug-ins installed on the early attack program whether the user is a trusted plug-in program for what it is not easy to judge. Current Internet-based programs that are being installed all the plug-ins are signed by the manufacturer's public key and the user based on it is generally reliable. This part of the user from the beginning phishing / Pharming attacks, then install the plug-in from the first problem. Installation of the plug-in and how to use your certificate on both sides of the user and the server can trust the device is needed. In addition, the server receives the plug from the perspective of the user, an attacker can determine whether the users of the line tools that should be provided. When you first install the plug- Plug-in ID to the server, so the server from the user and the attacker to get a way to figure out the distinction.

REFERENCES

[1] Y. Zhang, S. Egelman, L. Cranor, and J. Hong, "Phinding Phish: Evaluating Anti-Phishing Tools," Proceedings of the 14th Annual Network and Distributed System Security Symposium, Mar. 2007.

[2] G. Ollmann, The Phishing Guide, NGS Software Ltd., Sep. 2004.

[3] P.P. Swire, "Report from the National Consumers League Anti-Phishing Retreat," National Consumers Leage, Mar. 2006.

[4] G. Tally and R. Thomas, "Anti-Phishing: Best Practices for Institutions and Consumers," Anti-Phishng Working Group, pp. 8-20, Nov. 2004

[5]J.Stewart, "DNS Cache Poisoning - The Next Generation," LURHQ, pp. 1-13, Jan.2003.

[6] D. allan, "Identity Theft, Phishing and Pharming: Accountability & esponsibilities," OWASP AppSec, pp. 23-27, Oct. 2005.

[7] G. Ollmann, Security Best Practice: Host Naming and URL Conventions, NGS Software Ltd, pp. 5-6, Jan, 2005.

[8] L. Fette, "Learning to Detect Phishing Emails," Proceedings of the 16th International conference on World Wide Web, pp. 649-656, May, 2007.

[9] P. Kumaraguru, "Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System," SIGCHI conference on Human factors in computing systems, pp. 905-914, May 2007.

[10] M. Wu, "Do Security Toolbars Actually Prevent Phishing Attack?," SIGCHI conference on Human Factors in computing systems, pp. 601-610, Apr.2006.

[11] C. Karlof, "Dynamic Pharming attacks and locked same-origin pol icies for web browsers," Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 58-71, Oct. 2007.

[12] R. Dhamija, "Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks," Human Interactiv e Proofs, LNCS 3517, pp. 131-139, 2005.

저 자 소 개

홍 성 혁 (Sunghyuck Hong)

- 1995년 2월 : 명지대학교 컴퓨터 공학과 (공학사)
- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 교수

- E-Mail : shong@bu.ac.kr

<관심분야> : 네트워크 보안, 해킹, 센서네트워크 보안