의료정보 보호를 위한 피싱공격 확산방지모델 연구

최경호*, 정경용**, 신동근***

A Study of Prevention Model the Spread of Phishing Attack for Protection the Medical Information

Kyong-Ho Choi*, **Kyung-Yong Chung****, **Dong-Kun Shin*****

요 약 피싱 공격은 시간이 흐르면서 보다 더 지능적으로 실행되며, 기술적으로 고도화되고 있다. 해커는 지능화된 피싱 공격을 주요 기관의 내부 네트워크 침투를 위해 내부 사용자 컴퓨터를 점령하는 수단으로 이용하고 있다. 따라서, 본 연구에서는 고도화된 피싱 공격으로부터 내부 사용자와 중요 정보를 보호하기 위해 피싱공격 확산방지모델(PMPA : Prevention Model the spreading of Phishing Attack)을 기술하고자 한다. 내부 사용자들은 외부 웹메일 서비스와 내부 메일 서비스를 동시에 사용한다. 따라서 양 구간에서 발생하는 위협 요소를 동시에 식별하기 위해서는 각각의 패킷을 감시하고 저장하여 각각의 항목별로 구조화시켜야 한다. 이는 해커가 내부 사용자를 공격할 때 외부 웹메일 서비스와 내부 메일 서비스 중 어느 한 쪽을 이용하거나 또는 양쪽 모두를 이용할 수 있기 때문이다. 본 연구에서 제시된 모델은 기존에 연구된 메일 서버 중심의 보안구조 설계를 내부 사용자가 접속하는 내부 메일 서비스까지 보호할 수 있도록 확장한 것이며, 프록시 서버를 이용하여 직접 피싱 사이트 접속을 차단하는 것보다 메일 확인 시 해당 사이트를 목록화할 수 있기 때문에 별도의 요청/응답을 위한 대기 시간이 없다는 장점이 있다.

주제어 : 의료정보 보호, 피싱 공격, 유출 방지, 보안관리

Abstract Phishing attacks have been implemented in smarter, more advanced ways with the passage of time. Hackers use intelligent phishing attacks to take over computers and to penetrate internal networks in major organizations. So, in this paper, a model for a prevention of phishing attack spread is conceptual designed in order to protect internal users and sensitive or important information from sophisticated phishing attacks. Internal users simultaneously utilize both external web and organizational mail services. And hackers can take the both side equally as a vector. Thus, packets in each service must be monitored and stored to recognize threatening elements from both sides. The model designed in this paper extends the mail server based security structure used in conventional studies for the protection of Internet mail services accessed by intranet users. This model can build a list of phishing sites as the system checks e-mails compared to that of the method that directly intercepts accesses to phishing sites using a proxy server, so it represents no standby time for request and response processes.

Key Words : Medical Information Security, Phishing Attack, Prevention Leakage, Security Management

1. Introduction

The Internet allows access to information systems and financial transactions through personal IDs and passwords. If hackers steal such important information, they can access internal systems through networks and gain illegal profit. At this point, one of the methods used by hackers is phishing

본 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2012-0004478)
*Research Professor of Kyonggi University Center for Industry Security
**Professor of Sangji University, School of Computer Information Engineering
***Professor of Sahmyook University, Division of Computer (Corresponding Author)
논문접수: 논문접수: 2012년 4월 3일, 1차 수정을 거쳐, 심사완료: 2012년 4월 30일, 확정일: 2013년 3월 20일

attacks. Phishing attacks have been implemented in smarter and more advanced manners with the passage of time. Recently phishing has been targeted at groups as a type of targeted spear phishing with data gotten from social network sites such as Facebook and Twitter. These messages use the individual's name, organization division, e-mail, and even mobile phone number[4].

Hackers use such intelligent phishing attacks to dominate computers in order to penetrate internal networks in major organizations. It is difficult to guarantee the safety of Internet and internal networks from cyber attacks as long as intelligent phishing attacks continuously target specific enterprises or organizations. In addition, targeted spear phishing has been developed not only to steal personal information but also to modify personal computers in order to turn them into bases for penetrating a specific organization by distributing malicious code. As it is difficult to provide a proper response using spam filters for such an attack, a method that recognizes such a threat in advance and intercepts it through modeling a specialized security model is required. So in this paper, a Prevention Model for the spread of a Phishing Attacks (PMPA) is conceptual designed to protect intranet users and sensitive or important information from sophisticated phishing attacks.

2. Related Work

A security structure establishment based on Anti-Spam, Anti-Virus, and Anti-Phishing solutions has been used as a representative method for protecting users from phishing attacks. But the countermeasures based on formalized security solutions and technologies are not effective against sophisticated phishing attacks. Considering that the average lifetime of a specific phishing site is about 20 hours, instantaneous response to attacks is required[8][11].

A client-side defense mechanism that controls security configurations in web browsers or balloon tips can be used[1][9]. In this situation, there is a problem that users may access phishing sites by unfreezing their own security configurations, as hackers count on a user being tricked by similar domain names for web sites. A server-side defense mechanism could possibly verify emails using electronic signatures[6][7]. For instance, protecting users through e-mail can be possible by automatically removing links embedded in email text, "<a href=", as a server receives e-mails. However, it may cause some user inconveniences by removing linked large-capacity data or normal links, and it is not foolproof, because users can simply receive a text link in their email and copy/paste to visit the site. Although verifying the electronic signature method ensures a safe transactional relationship in such sites through trust between users and servers, it may present inconveniences to users in which they recognize individual security information provided by different sites. That is, it creates a difficulty in disturbing the use of information by transcending time and space. In addition, on the server manager side, a specific level of safety is to be continuously guaranteed, and there is a burden to prevent information exposure from hacking in order to sustain a reliable relationship between the two parties.

Although these countermeasures in server regions are effective to guarantee the safety of access for users who access services from external locations to internal servers, it shows a limitation in protecting internal members who access services from internal locations to external servers. It is due to the fact that the authorization for managing external servers is fully controlled by a security manager who controls corresponding servers.

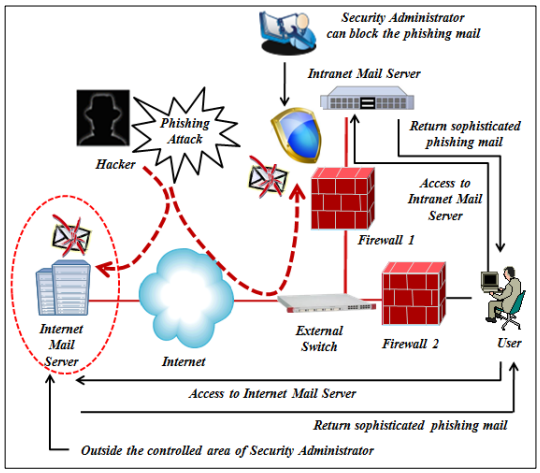
As mentioned above, a specialized, quick, and active security strategy for reacting to such sophisticated phishing attacks is required. In recent studies, such a requirement is reflected. Aycock determined two types of spear phishing attacks, as external and internal, and designed security structures for each property in an

attack[3]. OAK RIDGE Lab verified malicious domains using a proxy server as users accessed links included in e-mails in order to defend against spear or whale phishing, and compared the results with DNS inquires[12]. David developed SPEAD for blocking the penetration of cyber threats into user mail boxes by checking URLs and annexed files included in e-mails[5]. However, these methods can only protect users who use e-mail in a specific organization. Thus, it is necessary to design a security structure for protecting users from spear phishing and whaling attacks under a circumstance in which users do not use organization e-mails. The Detection System of SPA proposed in this study satisfies this requirement.

3. Consideration of PMPA

Members in enterprises or organizations receive lots of e-mails in the course of daily work. These e-mails include requests for the verification of facts, data, applications and communications with corresponding managers. Cyber threats can occur when checking these emails by connecting to phishing sites or downloading malicious code like trojans. Thus, such threats are to be detected and intercepted in advance.

In this case, intranet users use both external web and organizational mail services simultaneously. Thus, packets in each service are to be monitored and stored to recognize threatening elements on both sides, and that is to be structured for each item, because hackers use either the external web mail service or the organization's mail service or both sides as they attack intranet users. The situation that monitors both sides is caused by the location of the organization's mail server at a position of a DMZ[10]. Although the load of monitoring and storing packets is decreased, since the internal member and organization's mail server are located in the same network region, it will cause a problem of detecting attacks implemented by internal members using an organization's mail services. Thus, the network region used by the internal member and organization's mail server is to be operated as a separate way for establishing a security structure for sophisticated phishing attacks.



[Fig. 1] Typical user e-mail environment

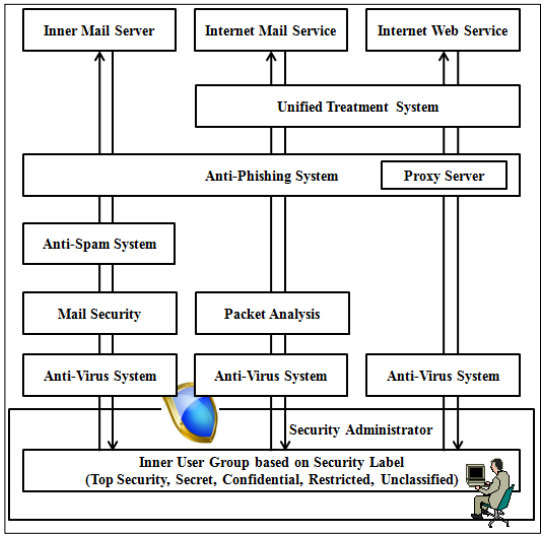
4. Conceptual design of PMPA

For security managers, it requires greater concentration of sophisticated phishing attacks as a higher level threat than others, because a single leak of information will cause a huge amount of damage. In this context, sophisticated phishing attacks that target internal members in an organization through e-mails are considered. Then, a security structure that checks all incoming e-mails to internal networks is established. Work operated by establishing such a structure for using e-mail can be classified as follows:

- ❍ E-mails are perused by internal or external mail servers at internal networks.
- ❍ E-mails are perused by internal mail servers at external networks.

Thus, the conceptual designed PMPA collects packets generated in both mail server and user regions separately by copying the packets, in order to extract the packets through traffic monitoring occurring in these two situations. Then,

- All mail delivered to the inner mail servers are checked by the security solution regardless of whether or not these mails are perused.
- Mail delivered to the Internet mail service is not flown to the inner before perusing the mails by the owners of accounts. However, as users check e-mails using an internally-operated information system, sophisticated phishing attacks can be detected and blocked by screening traffic introduced from external networks to internal networks.



[Fig. 2] A conceptual design of the PMPA

In addition, the PMPA structure is based on Anti-Spam, Anti-Virus, Intrusion Prevention System and Unified Treatment System. Because hackers are now able to simulate the detection of attacks using the same products and technologies as the products and technologies used in the target, they represent helplessness against cyber threats before updating to recent security policies. For instance, it is difficult to react to a Zero-Day Attack that is a serious recently-occurring threats[2]. Also, as a general security policy is applied to such security products and technologies, it is difficult to perform individual and serious defenses. However, it should complement the PMPA against known attacks.

5. Discussion and Future Work

The PMPA conceptual design in this paper extends mail server-based security structure used in conventional studies to the protection of Internet mail services accessed by intranet users. Because it can build a list of phishing sites as the system checks e-mails, it requires no standby time for the requesting and responding process. However, it is difficult to perform a defense against internal attack within internal networks because a test for a blocklist can be allowed. Also, it shows some disadvantages in using the method together with Anti-Spam and Anti-Virus and requires an additional intrusion prevention function for intercepting accesses to phishing sites. Thus, the model conceptual designed in this study can be used in more than a specific level of group or organization. In addition, it is necessary to periodically update the proposed system, because it cannot recognize e-mails as long as the packet information of the Internet mail services is not provided. And the interception time of sophisticated phishing attacks can be varied based on the configured threshold, depending on the security label of users, because there are some cases that the recognition of service types are difficult due to the large number of Internet sites. Therefore, it is necessary to exactly quantify the decision of security levels and the scale of work correlation in order to stably operate the unit modules applied to the conceptually-designed model.

Finally, it should be noted that white and well-reputed domains can be used to distribute phishing mails and malicious code through hacking them. In this case, it is desirable that the white and well-reputed domains are to be managed as an integrated list for verifying possible phishing threats, and the list is to be updated as new hacking or phishing sites are found.

References

[1] A. Sagar, "Phishing Attacks and Counter-Measures", CERT-In White Paper, Indian Computer Emergency Response Team Enhancing Cyber Security in India, 2005.

[2] A. Patcha, P. Jung-Min, "An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends, Computer Networks, Vol. 51, No. 12, pp. 3448-3470, 2007.

[3] J. Aycock, "A Design for an Anti-Spear-Phishing System", Virus Bulletin Conference, pp. 290-293, 2007.

[4] B. Parmar, "Protecting Against Spear-Phishing", Computer Fraud & Security, Vol. 2012, Issue 1, pp. 8-11, 2012.

[5] D. T. Merritt, "Spear Phishing Attack Detection", Degree of Master of Science in Computer Engineering Thesis, Air Force Institute of Technology, Air University, 2011.

[6] D. H. Lee, K. H. Choi, K. J. Kim, "Intelligence Report and the Analysis Against the Phishing Attack Which Uses a Social Engineering Technique", ICCSA'07, LNCS 4706, pp. 181-192, 2007.

[7] G. Ollmann, "The Phishing Guide : Under- standing & Preventing Phishing Attacks", IBM Internet Security Systems, 2007.

[8] H. R. Kim, J. H. Jeoung, S. P. Hong, "Design and Implement to Prevention from Personal Information abuse in Web Environment", Korean Society for Internet Information, Vol. 9, No. 2, pp. 151-156, 2008.

[9] J. H. Kim, Y. J. Maeng, D. H. Nyang, K. H. Lee, "Congnitive Approach to Anti-Phishing and Anti-Pharming", J. of Korea Institute of Information Security and Cryptology, Vol. 19, No. 1, pp. 113-124, 2009.

[10] S. Preda, F. Cuppens, Nora Cuppens-Boulahia, J. Garcia-Alfaro, L. Toutain, "Dynamic Deployment of Context-Aware Access Control Policies for Constrained Security Devices", J. of Systems and Software, Vol. 84, No. 7, pp. 1144-1159, 2011.

[11] T. Moore, R. Clayton, "Examining the Impact of Website Take-down on Phishing", Proc. of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit, ACM, 2007.

[12] Anti-Phishing and Whaling, Cyberspace Sciences and Information Intelligence Research Group Projects, Computational Sciences & Engineering Division, OAK RIDGE National Lab.

Kyong-Ho Choi

- 2002. 2, Kyonggi University Economics (B. S.)
- 2005. 2, Kyonggi University Economics (M. S.)
- 2008. 2, Kyonggi University Information Security (Ph. D.)
- 2012. 3~Current, Research Professor of Kyonggi University, Center for Industry Security
- Interesting Area : Security Architecture, Security Policy
- E-mail : cyberckh@gmail.com

Kyung-Yong Chung

- 2000. 2, Inha University Dept. of Computer Information Engineering(B. S)
- 2002. 2, Inha University Dept. of Computer Information Engineering(M. S)
- 2005. 5 Inha University Dept of Computer Information Engineering(Ph. D)
- 2006. 3 ~ Current, Professor of Sangji University Dept. of Computer Information Engineering
- Interesting Area : Data Mining, Security, HCI
- E-mail : dragonhci@hanmail.net

Dong-Kun Shin

- 1986 2, Inha University Dept. of Computer Information Engineering(B. S)
- 1995. 2, Dongguk University Dept. of Computer Information Engineering(M. S)
- 2010. 2, Inha University Dept of Computer Information Engineering(Ph. D)
- 2006. 3~Current, Professor of Samyook University Division of Computer
- Interesting Area : Data Mining, Security, HCI, SE
- E-mail : dkshin@hanmail.net