피싱 공격에 대한 사용자 정보보호 방안

김정태
목원대학교

Technique of Information Security for Users against Phishing Attacks

Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

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. This paper presents a novel browser extension, AntiPhish, that aims to protect users against spoofed web site-based phishing attacks. To this end, AntiPhish tracks the sensitive information of a user and generates warnings whenever the user attempts to give away this information to a web site today requires only the server to be hat is considered untrusted.

Ⅰ. Introduction

Phishing was first reported when America Online users were lured in the mid 1990's by phishers to part with their user names and passwords. One intrusion technique used by phishers is the deployment of worms. The W32.Mimail.I and W32.Mimail.S worms attempted to fool users into handing over credit-card information while posing as either a PayPal application or Microsoft Windows expiration notice. There are various guidelines for prevention of phishing attacks. The Anti-Phishing Working Group frequently publishes reports on phishing activities. Victims of identity theft may use the APWG's web-site to report phishing attacks. The newest strategy that financial services implement in prevention of phishing attacks is the verification of financial transactions via mobile technology. One of the latest computer-related problems to arise is phishing, in which e-mails lure unsuspecting victims into giving up user names, passwords, Social Security numbers, and account information after linking to counterfeit bank, credit card, and e-commerce Web sites. Currently, SSL and TLS rely on Public Key Infrastructure (PKI) for users and servers to authenticate each other.

In PKI, a trusted third party known as the Certification Authority (CA) will sign a digital certificate binding the public key of an entity to its identity. The public key of an entity is authenticated if the signature verification of the digital certificate with the CA's public key is valid. SSL implementation authenticated. However, there have been reported cases of certificates being issued to phisher's web server and certificates falsely issued to unauthorized individuals, hence attackers with these falsely issued certificates can easily launch phishing attacks to impersonate the legitimate web site.

II. Related Work

Two similar, browser-based plug-in solutions exist to mitigate Phishing attacks . Both solutions are from Stanford university. PwdHashis an Internet Explorer plug-in that transparently converts a user's password into a domain-specific password so that the user can safely use the same password on multiple web sites. A side-effect of the tool is some protection from phishing attacks. Because the generated password is domain specific, the password that is phished is not useful. The problem, however, is that the solution only works for protecting passwords and does not work for sensitive information. Unfortunately, phishing attacks are also becoming more sophisticated. In June, a PayPal phishing attack was discovered that used a cross-site scripting vulnerability in PayPal's Web site to display what appeared to be an authentic Web page—one hosted on the paypal.com domain and protected by Transport Layer Security (TLS) with a valid certificate—that informed users their accounts were disabled and then took them to a new page in which they were to enter their personal information (http://news.netcraft.com/archives/2006/06/16/paypal_security_flaw_allows_identity_theft.html). Such an attack is almost impossible for the average user to detect. The domain in the address bar is correct, and the lock icon in the Web browser indicates that everything is fine.

III. Types of phishing attacks

3.1 Spoofing e-mails and web sites

Many phishing attacks now rely on a more sophisticated combination of spoofed e-mails and web sites to steal information from victims. Such attacks are the most common form of phishing attacks today. In a typical attack, the attackers send a large number of spoofed e-mails that appear to be coming from a legitimate organization such as a bank to random users and urge them to update their personal information.

3.2 Exploit-based phishing attacks

To mitigate exploit based phishing attacks (as well as other security threats that are directly related to browser security such as worms, trojans and spyware), browser manufacturers need to make sure that their software is bug-free and that users are up to date on the latest security fixes.

IV. Methods of Attacking Phishing

Several antiphishing approaches are becoming popular. One key to many of these approaches is having Internet service providers (ISPs) close phishing Web sites. phishers. The most straightforward way for a phisher to scam people is to make the phishing Web pages similar to their targets.

A phishing strategy includes both Web link obfuscation and Web page obfuscation. Web link obfuscation can be carried out in four basic ways:

1. adding a suffix to a domain name of the URL,
2. using an actual link different from the visible link,
3. utilizing system bugs in real Web sites to redirect the link to the phishing Web pages
4. using cousin domain names (e.g., replacing certain characters in the target URL with similar characters).

The Web page obfuscation can be carried

out in three basic ways:

1. using the downloaded Web page from the real Web site to make the phishing Web page appear and react exactly the same as the real one does
2. using a script or images to cover the address bar to scam users into believing they have entered the correct Web sites
3. using visual-based content (Image, Flash, JavaApplet, etc.) rather than HTML to avoid HTML-based phishing detection.

The Antiphishing Database Server is the center for registration of legitimated Web sites which want protection, and maintains a phishing link list. It also acts logically as a part of the Antiphishing Proxy to preprocess protected Web pages, such that this design makes good system scalability. The registered legitimate Web pages are preprocessed in advance, and their signatures are saved in the database. The owner of the protected Web page can specify a set of sensitive keywords (e.g., "eBay" for www.ebay.com) during registration to the Antiphishing Database Server, which are used for checking the e-mails. Antiphishing Proxy synchronizes the database from the Antiphishing Database Server.

To deploy the proposed phishing detector in a browser, a user downloads a plug-in comprising both an identity extractor and a page classifier from a trusted server. Note that such a server is not necessarily globally trusted. For example, it can be a server within the user's organization. The plug-in should be trained by the server before it is provided to the users. Once downloaded, the plug-in functions independently without involvement of any third party. The architecture of our scheme is shown in Figure 2.

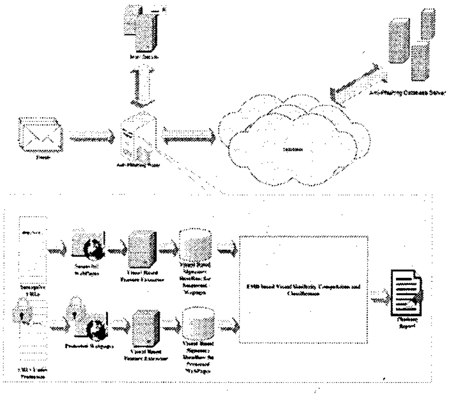

Fig. 1 Architecture of the antiphishing system.

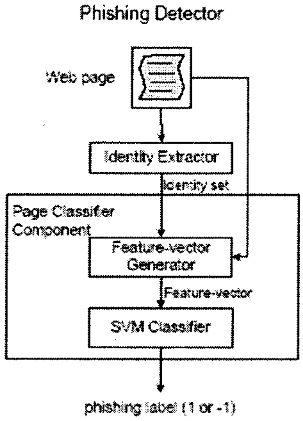

Fig. 2 Architecture of the phishing detector

When a browser opens a web page, an identity is extracted by the identity extractor and the structural features of the page are extracted and converted into vectors. The SVM-based page classifier, which has been trained offline, takes the vectors as an input and outputs a phishing label.

The Web page obfuscation can be carried out in three basic ways:

1. using the downloaded Web page from

the real Web site to make the phishing Web page appear and react exactly the same as the real one does,

2. using a script or images to cover the address bar to scam users into believing they have entered the correct Web sites, and
3. using visual-based content (Image, Flash, JavaApplet, etc.) rather than HTML to avoid HTML-based phishing detection.

V. Procedure of Phishing Attacks

In general, phishing attacks are performed with the following four steps:

1) Phishers set up a counterfeited Web site which looks exactly like the legitimate Web site, including setting up the web server, applying the DNS server name, and creating the web pages similar to the destination Web site, etc.

2) Send large amount of spoofed e-mails to target users in the name of those legitimate companies and organizations, trying to convince the potential victims to visit their Web sites.

3) Receivers receive the e-mail, open it, click the spoofed hyperlink in the e-mail, and input the required information.

4) Phishers steal the personal information and perform
their fraud such as transferring money from the victims' account.

More advanced technical attacks move away from social engineering tactics and into the realm of malicious software. Malware attacks comprise the installation and execution of malicious software on a victim's personal computer. In a hybrid approach a phisher will use social engineering tactics to lure a user into opening or downloading a file that contains a malicious software installation. Security vulnerabilities are also exploited to install malicious software on an unsuspecting user's computer. Phishing attacks are on the rise and becoming increasingly complex.

V. Conclusion

This paper presents a novel browser extension called AntiPhish that aims to protect users against spoofed web site-based phishing attacks. AntiPhish tracks the sensitive information of a user and generates warnings whenever the user attempts to transmit this information to a web site that is considered untrusted.

References

[1] http://www.anti-phishing.org, 2004.

[2] http://www.verisign.com/verisign-businesssolutions/anti-phishing-solutions/, 2005.

[3] E.W. Felten and J.A. Halderman, "Digital Rights Management, Spyware, and Security," IEEE Security & Privacy, vol. 3, no. 6, pp. 18 - 23.

[4] Kirda E., Kruegel C.,"Filching Attack of on-line Status", Journal, Network Security Technology and Application, Vol. 6, No. 4, 2005, pp. 17-20.

[5] PhishGuard.com. Protect Against Internet Phishing Scams http://www.phishguard.com/.

[6] C. L. Schuba, "Analysis of a denial of service attack on TCP,"*IEEE Security and Privacy Conference*, 1997, pp. 208-223.