ISBN: 978-93-83758-09-8

Security Against Phishing Techniques Through a Web Based User Interface

[1]Priya Dhingra, [2]Anshul Arora
[1,2] Student, M.Tech., Computer Science, Geeta Engineering college, Naultha (Panipat)
[1] pdpriya9@gmail.com,
[2] anshul.arora018@gmail.com

Abstract: Phishing is a technique of online theft of the personal information of user that includes his bank account number or Credit Card number. This paper provides the details of phishing techniques and the various types of attacks that can lead to loss of personal information. Various anti phishing solutions have been discussed that includes digital signature and deactivating JavaScript for HTML enabled text elements. This paper presents AntiPhish, a browser extension that aims to protect inexperienced users against spoofed web site-based phishing attacks. AntiPhish employs cryptography and DES algorithm for successful encryption of the confidential information.

***Keywords*: Phishing, Anti-sh, JavaScript, ES, Plug- ins**

I. INTRODUCTION

As far as people with criminal intentions are concerned, identity theft is an old idea. Phishing is a brand spoofing variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting. Phishing is a form of online criminal trick of stealing victims' personal information by sending them spoofed emails urging them to visit a forged webpage that looks like a true one. Phishing is a form of online identity theft Specifically, phishers attempt to trick Internet users into revealing sensitive or private information, such as their bank account, credit-card numbers and passwords.

The Phishing process involves an attacker sending fraud mail to the consumer ,which replies with its personal information to the attacker impersonating him as the official website. The attacker then uses this personal Information for financial frauds.

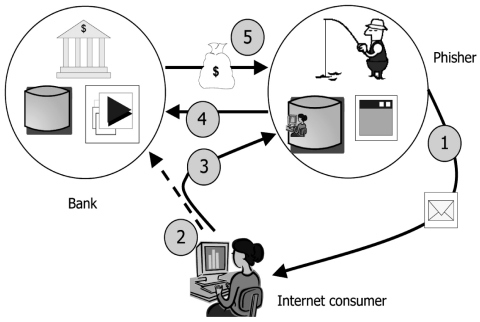

Fig:1 Illustration of Phishing Procedure

II. PHISHING TECHNIQUES

In this section, we give a brief overview of the different types of phishing attacks to familiarize the reader with the threat.

Social Engineering: Social Engineering is a type of intrusion depends on human interaction whereby victims are tricked into revealing their confidential information by breaking security procedures. An attacker conducting a social engineering attack on a network attempts to gain the confidence of an authorized user of that network to get them to reveal sensitive information. This can be achieved by messaging the authorized user of some urgent problem that needs to be solved immediately.

Basic URL Obfuscation/Web Spoofing: URL obfuscation misleads the victims into thinking that a link and/or web site displayed in their web browser or HTML capable email client is that of a trusted site. These methods tend to be technically simple yet highly effective, and are still used to some extent in phishing emails today.

*Simple HTML redirection :*One of the simplest techniques for obscuring the actual destination of a hyperlink is to use a legitimate URL within an anchor element but have its href attribute point to a malicious site. Thus clicking on a legitimate-looking URL actually sends the user to a phishing site.

Use of JPEG images: Electronic mail rendered in HTML format is becoming more prevalent. Phishers are taking advantage of this by constructing phishing emails that contain a single image in JPEG format. When displayed, this image appears to be legitimate email from an online bank or

ISBN: 978-93-83758-09-8

merchant site. The image often includes official logos and text to add to the deception. However, when users click on this image, they are directed to a phishing site.

Registration of similar domain names
At initial glance, users may attempt to verify that the address displayed in the address or status bar of their web browser is the one for a legitimate site. Phishers often register domain names that contain the name of their target institution to trick customers who are satisfied by just seeing a legitimate name appear in a URL .A widely implemented version of this attack uses parts of a legitimate URL to form a new domain name as demonstrated below:

Legitimate URL http://login.example.com
Malicious URL http://login-example.com

Emails Spoofing
The most common phishing tool is emails and links to compromised web sites that have the look and feel of trusted brands.

Cross-site scripting attacks
These attacks are popular with websites that accept user input. For e.g. a phisher can put up an obfuscated code on a benign commerce site. The URL to this site thus contains both the original code and the obfuscated one such as some JavaScript that targets the sensitive user information. An example of this would be recording user input data (username and password) that the user enters, record them and then forward the user to the original site. This can give messages such as Incorrect password making the user feel that he typed in the wrong data.

Man-In-The-Middle Attacks
Man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker. The man-in-the-middle attack can be staged using shared media by configuring the network interface in promiscuous mode.

III. THE PHISHING PROCESS

Most phishing attacks take four distinct steps toward defrauding unwary recipients:

(1) The scam operators setup the phishing website. This website usually imitates an established, legitimate site;
(2) Using guessed or copied email addresses, the scammers send out emails purporting to come from the legitimate site;
(3) the recipient downloads their email and receives the phishing message. The email asks the user to click on a hyperlink and enter personal details on the resulting website. If the user clicks on the hyperlink the phishing site will be displayed. If duped, the user may then enter the requested personal information;
(4) the recipient's personal details are now held by the scam operators. The scammers may now assume the identity of the recipient and gain illicit access to funds.

IV. ANTI-PHISHING SOLUTIONS

Digitally Signed Email
Digitally signed emails allow the recipient to verify that the sender information is genuine. This also lets the recipient know that the message has not been modified in transit.Popular digital signature standards include OpenPGP and S/MIME, although they are incompatible with each other. These facilities can be used with mail clients such as Outlook, Navigator and Eudora. At first glance, digitally signed emails appear well suited to combating the phishing problem. However, to date very few organizations with on-line banking or e-commerce facilities use this technology.

Online Brand Monitoring
Companies such as Cyveillance, NameProtect and Netcraft offer on-line brand monitoring services. This entails monitoring domain name registrations, web pages, spam emails and other on-line content for illegal use of clients' brand names. If illegal use of a client's brand name is detected, for example on a phishing website, then the client is notified and can take remedial to close the website.

Spam Filters
Current spam filters can be used to defend end-users against phishing attacks. Spam filters classify incoming mail as either spam or non-spam. Filters of this type judge email once it has been download from the mail server. Spam emails are often removed by filters, and no spam may be present when the end-user views or downloads their mail.To achieve this, most spam filters use Bayesian filtering techniques. Bayesian filtering allows the filter to 'learn' and adapt over time, taking into account the latest spam emails and the user's personal preferences.Many users may not even be aware that spam filters exist. For such reasons, spam filters cannot be considered a complete solution to phishing emails.

Web browser extensions
Since phishing relies largely on deceptive Web sites, Web browsers are a natural focus for anti-phishng measures. An early means of adding anti-phishing capabilities to Internet Explorer was the Earthlink Toolbar.Whenever the user browses to a known phishing web site, the tool alerts them to this fact and the user is redirected to a warning page hosted by Earthlink (Earthlink, 2006). Similar strategies for user alerting are now appearing within mainstream Web browsers. Mozilla Firefox has a facility enabled by default that also works by checking visited Web sites against a list of known phishing sites. In this case, the phishing site list is automatically downloaded and regularly updated within Firefox. Microsoft have also added comparable anti-phishing features to version 7 of Internet Explorer. Such anti-phishing extensions to Web browsers help by alerting users to known phishing sites. This relies on a current database of phishing website information. A system designed in this way cannot

ISBN: 978-93-83758-09-8

protect against all phishing attacks, since there will always be a delay between a phishing attack going live and the database being updated. During this delay users are not protected from the new phishing attack.

V. THE ANTI-PHISHING WEB SERVICE

Anti-Phishing Web Service (APWS) analyses users'emails and advises if they are likely phishing attempts.
The APWS operates in a three step process:
(1) Users forward any suspect email to the APWS for analysis;
(2) The APWS performs a series of tests on the email,each resulting in a score. An overall score is derived which indicates a likelihood that the email is a phishing attempt;
(3) The APWS generates an online report for the user.

A phishing risk rating is assigned according to the total score for the email (Table 1).

Table 1: Phishing risk rating

Total Score	Risk Rating
3 or more	Very High
2	High
1	Moderate
0	Low

This test is performed on every URL and returns true if the Levenshtein Distance (LD) between the organization domain and the purported sender's organization domain is less than half the length of the purported sender's organization domain. We do not return true if the LD in this calculation is zero (i.e. the domains being compared are equal).

Phishing emails often contain anchor tags wherein the text the anchor text resembles a URL, but that URL points to a different location than the tag's 'href' attribute. We returns a positive increment for URLs with such a feature. Finally, we check for attachments with malicious content. This test is performed on every attachment object and returns a positive increment if the attached file name extension matches one of the following: ade, adp, bas, bat, chm, cmd, com, cpl, crt, exe, hlp, hta, inf, ins, isp, js, jse, lnk, mdb, mde, msc,msi, msp, mst, pcd, pif, reg, scr, sct, shs, url, vb, vbe, vbs, wsc, wsf and wsh.

Figure 1. Part of a real phishing e-mail that tries to lure the victim into giving away sensitive personal information.

Antiphish

AntiPhish is an application that is integrated into the web browser. It keeps track of a user's sensitive information (e.g., a password) and prevents this information from being passed to a website that is not considered "trusted" (i.e., "safe").This content is protected by a *master password*. Once this password is entered by the user, a login form that has previously been saved, for example, will automatically be filled by the browser whenever it is accessed. Antiphish takes this common functionality one step further and tracks *where* this information is sent.

Figure 3 shows the right-click pop-up menu in the browser with the integrated AntiPhish menu items. After AntiPhish is installed, the browser of type *password* are captured and cached.Besides storing the sensitive information, AntiPhish also stores a mapping of where this information "belongs" to. That is, the domain of the web site where this information was originally entered is also stored.

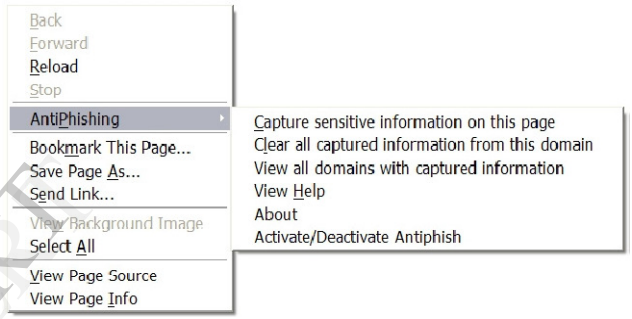

Figure 3. The AntiPhish application menu integrated into the browser.

prompts a request for a new master password when the user enters input into a form for the first time. After this password is entered, the AntiPhish menu can be used to capture and store sensitive information. The master password is used to encrypt the sensitive information before it is stored. The symmetric DES algorithm is used for the encryption and decryption.

In the DES Algorithm there are two main types of cryptography.
1.) Symmetric key or secret key cryptography is the oldest type whereas asymmetric or public key cryptography is only being used publicly since the late 1970's.
2.) Asymmetric cryptography was a major milestone in the search for a perfect encryption scheme. Secret key cryptography goes back to at least Egyptian times and is of concern here. It involves the use of only one key which is used for both encryption and decryption.

In our current implementation, user interaction is needed to tell AntiPhish that a piece of informationon a page is important and that it should be protected against phishing attempts. After the user enters sensitive information such as a password, the AntiPhish menu is used to scan the page and to capture and store this information. If AntiPhish detects, for example, that the user has typed his online banking password into a text field on a web site that is not in the online banking

web site domain (i.e., an "untrusted" web site), then it generates an alert and redirects to an information page about phishing attacks.

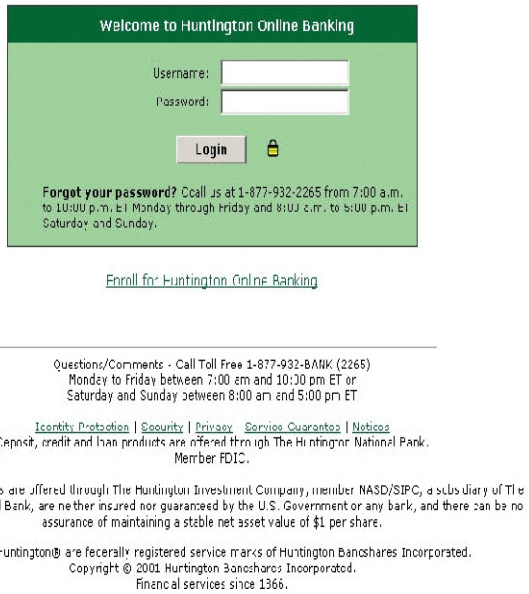

Figure 2. Screenshot of the spoofed Hunting online banking page. The login screen closely resembles the legitimate login page.

Controlling the sensitive information flow

As far as AntiPhish is concerned, every page that contains a form is a potential phishing page.AntiPhish is activated every time the user presses a key, loads a new page, clicks the mouse or has the current focus on a text element (i.e., text field or text area).

Possible ways of by-passing antiphish with javascript

As long as the web page that the user is viewing is pure HTML, AntiPhish can easily mitigate phishing attacks. This is because the attacker can only steal the sensitive information in the page after the user performs a submit. Before this can happen, however, AntiPhish detects that sensitive information has been typed into a form and cancels the operation. Stopping a phishing attack in an HTML page that has Javascript, on the other hand, is not that easy and special care has to be taken Instead of waiting for the user to press a submit button to send the information, the attacker could intercept the keys that are pressed and send the information character by character to a server of his choice. Typically, this is done by modifying the URL of an existing or hidden image to a web site that the attacker controls (e.g., if "a" has been pressed, an image URL may be set to *http://attacker.com/key?a*). Another possibility for the attacker could be to set a simple timer and to capture "snapshots" of the information in the forms. In this way, an important part of the information could be captured without the user ever hitting a submit button.

The solution we use in AntiPhish is to *deactivate* Javascript every time the focus is on an HTML text element and to *reactivate* it whenever the focus is lost. Using this technique, we ensure that the attacker is not able to create hooks, timers and intercept browser events such as key presses while the user is typing information into a text field. At the same time, we ensure that the legitimate Javascript functionality on a page(e.g., such as input validation routines) are preserved.

By the time the focus is lost from the text Element and JavaScript is reactivated, AntiPhish has already determined if the information that was typed into the text element is sensitive. If the web site is untrusted, the operation can be canceled. One side-effect of our approach is that legitimate event-based JavaScript functionality such as input validation based on key presses will not function. The use of key press events for input validation, however, is uncommon. Most web sites perform client-side input validation once before a form is submitted.

VI. IMPLEMENTATION DETAILS

- We implemented the prototype of AntiPhish as a Mozilla browser extension (i.e.,plug-in) Mozilla browser extensions are written using the Mozilla XML User-Interface language (XUL) and JavaScript. The Mozilla implementation of AntiPhish has a small footprint and consists of about 900 lines of Javascript code and 200 lines of XUL user interface code. We used Paul Tero's Javascript DES implementation for safely storing the sensitive information.

- If the user has been attacked by phishing site that asks for user id and password.When the victim starts typing in heruser ID, she is prompted for the master password.The master password is then used to decrypt the stored sensitive information.

After typing in her user ID, the victim clicks the password text field and starts typing the password. After the last character of the password is entered, an alert messageis displayed telling him that he is a potential victim of a phishing attempt because the sensitive information he used on his site is about to be passed to the untrusted site (Figure 4).

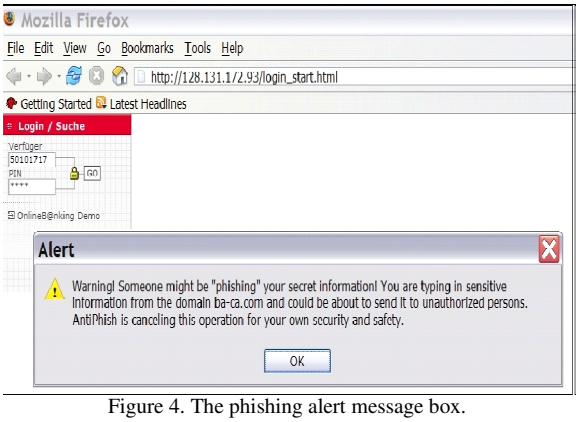

Figure 4. The phishing alert message box.

VII. CONCLUSIONS

Attackers are employing a large number of technical spoofing tricks such as URL obfuscation and hidden elements to make

ISBN: 978-93-83758-09-8

a phishing web site look authentic to the victims. The most effective solution to phishing is training users not to blindly follow links to web sites where they have to enter sensitive information such as passwords and industry to provide solutions for the phishing threat. 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.It is believed that AntiPhish is a step in the right direction and a useful contribution for protecting users against spoofed web site-based phishing attacks.

VIII. REFERENCES

[1] Blake Ross, Collin Jackson, Nick Miyake, Dan Boneh and John C. Mitchell. A Browser PlugIn Solution to the Unique Password Problem. http://crypto.stanford.edu/PwdHash/, 2005.

[2] Gunter Ollman. The Phishing Guide – Understanding and Preventing Phishing Attacks. White Paper, Next Generation Security Software Ltd.,2004.

[3] Heise Security. German Interior Minister Schily requests protection against online scams. http://www.heise.de/security/, 2005.

[4] The Anti-Phishing Working Group ,"APWG Phishing Trends Reports, [Online] Available : www.antiphishing.org/ phishReports Archive.html

[5] Jason Milletary, "Technical Trends in Phishing Attacks",Carnegie Mellon University,2005
[6] Sumit Siddharth, "Anti Spamming Techniques.pdf".

[7] SpoofGuard. Client-side defense against webbased identity theft. http://crypto.stanford.edu/SpoofGuard/, 2005.

[8] The Antiphishing Working Group. Home Page. http://www.anti-phishing.org, 2004.

[9] Mozilla Extensions. Home Page. http://update.mozilla.org/extensions/, 2005.

[10] Gunter Ollman. The Phishing Guide – Understanding and Preventing Phishing Attacks. White Paper, Next Generation Security Software Ltd., 2004.

[11]Gunter Ollmann, *"The Phishing Guide"* - NGS White Paper http://www.ngssoftware.com/papers/NISR-WP Phishing.pdf

[12]David Watson,Thorsten holz,Sven Mueller, *"Know Your Enemy: Phishing"* http://www.honeynet.org/papers/phishing/

[13] Jason Milletary, *"Technical Trends in Phishing Attacks"*www.uscert.gov/reading_room/phishing_trends0511.pdf