Custom Plugin – A Solution to Phishing and Pharming Attacks

Omer Mahmood
School of Information Technology
Charles Darwin University
Darwin, NT, Australia

Abstract - *This paper proposes a new method to detect, alert and protect the user from Internationalized Domain Names [1] (IDN) and Uniform Resource Locator (URL) spoofing, phishing, pharming and man-in-the-middle attacks by validating the site before the user actually enters the personal details. The suggested method is based on the use of a browser plugin which enables the user to validate the website which provides visual feedback. In case of pharming, where Domain Name System (DNS) is hijacked, the plugin automatically notifies the user of possible attack, posts the attack information to the server and redirects the user to legitimate website. SSL/TLS [2] certificates are also automatically checked, verified and validated by the plugin in order to check for man-in-the-middle and pharming attacks.*

Keywords: Phishing, Pharming, Browser Based Attack Prevention.

1 Introduction

Phishing, also referred as “password harvesting fishing”, is an act of attempting to deceptively collect personal information in order to steal person’s identity, mostly by using email which appears to have come from legitimate business. Such emails are commonly known as hoax emails. Hoax emails are used to deceive the recipients into revealing personal information for example passwords or credit card details. Phishing attacks are leading cause of account hijacking in US and Australia. For example Westpac [3], a major Australia bank, has warnings on the main page regarding phishing and hoax emails with hoax example emails [4]. Most methods of phishing use some form of technical deception designed to make a links in an email appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phishers, such as http://www.yourbank.com.example.com/. Another method of spoofing links used web addresses containing the '@' symbol, which were used to include a username and password in a web URL (contrary to URL standard [5]). For example, the link http://www.yahoo.com@youAreHappy.com/ might deceive an individual into believing that the link will open a page on www.yahoo.com, whereas the link actually directs the browser to a page on youAreHappy.com, using a username of www.yahoo.com; were there no such user, the page would open normally. This method has since been closed off in the Mozilla [6] and Internet Explorer [7] web browsers. The problem further aggravates because mostly people tend to use the same password for multiple websites. Thus if one password is lost, all sites are compromised. According to Gartner [8] “more than 1.4 million users have suffered from identity theft fraud, costing banks and card issuers $1.2 billion in direct losses in the past year” i.e. 2004. The number of unique phishing websites detected by Anti-Phishing Working Group was 9715 in January 2006, a huge increase in unique phishing sites from the previous two months e.g. in November 4630 unique phishing websites were detected [9]. Unlike phishing where individuals are deceived through hoax emails, in pharming DNS Servers are attacked. In pharming the hacker acquires the Domain Name for a particular site and redirects the user to different IP address where the fake website is hosted. Pharming results in even greater financial loss as large number of users are redirected to bogus websites even when they enter correct URL. Although pharming is new application of well-known security weaknesses but it can be addressed with better browser security implementation and digital certificates. In order to address phishing and pharming attacks, a solution is required which enables the user to verify the website they are currently viewing before they enter the personal information. This paper proposes a new method which makes use of a browser plugin that provides site verification service to the end user where the user has pre-established relationship with the organisation whose site is being visited. The plugin first checks for IDN followed by comparison of IP address of currently opened website with the locally stored IP address range of the organisation along with verification and validation of website’s digital certificate in order to determine the legitimacy of the website. The rest of the paper is organized as follows. Section 2 discusses some of the related but different solutions, whereas section 3 covers their limitations and shortcomings. In Section 4 the detailed architecture of the proposed solution is presented, which is followed by the conclusion in Section 5.

2 Currently Available Solutions

There are three readily available solutions which provide site verification functionality to some extent. This section outlines brief architecture of all three solutions.

2.1 Microsoft Phishing Filter [10]

Microsoft Phishing Filter is freely available as an add-in for MSN Search Toolbar [11] and is also built into Internet Explorer 7 Beta 2 Preview [12]. MS Phishing Filter checks the address of the Web site user visits against the list of Web site addresses stored on the user computer that have been reported to Microsoft as legitimate ("legitimate list"). When the user visits a website for the first time that is not on the legitimate list, the user is prompted whether the Phishing Filter should automatically check all visited Web sites. If the user opts for automatic checking then, addresses not on the legitimate list will be sent to Microsoft and checked against a frequently updated list of Web sites that have been reported to Microsoft as phishing, suspicious, or legitimate Web sites. Phishing Filter sends the current and previously visited Web sites to Microsoft, together with some standard information from the user computer such as IP address, browser type, and Phishing Filter version number. However in order to protect the privacy of the user, the address information sent to Microsoft is encrypted using SSL and limited to the domain and path of the web site including other information that associated with the address, such as search terms, data you entered in forms, or cookies, will not be sent [13]. All the data sent to Microsoft for site checking is real-time because this offers better protection than only using static lists. This technique also avoids overloading of networks.

2.2 EarthLink Toolbar [14]

The free browser toolbar provided by EarthLink (http://www.earthlink.net/) can be installed in Microsoft Internet Explorer and Mozilla Firefox [15]. The toolbar comes with the ScamBlocker which provides two levels of protection:

2.2.1 ScamBlocker automatically alerts the user about the legitimacy of the site before they view the webpage, if it is on the list of known phishers which is maintained by EarthLink.

2.2.2 ScamBlocker gives the user real-time fraud analysis of all Web sites they visit. The ScamBlocker icon on EarthLink Toolbar changes to visually notify the user if they have landed on a potentially dangerous site.

2.3 PassMark Two-Factor Two-Way Authentication

PassMark Security [16] provides commercial service to financial institutions and organisations. Their solution provides site and email verification service by reversing the polarity of traditional authentication approach where the website is authenticated to the user before the user enters the personal details; without any installation of new software or hardware on user’s computer. PassMark is data which is unique to each individual user and is displayed on the webpage before the user logs into the website. The user is required to select an image when they first register with the institution. Upon registration a unique device ID is generated, like a secure cookie, to identify the computer from which the PassMark is being requested.

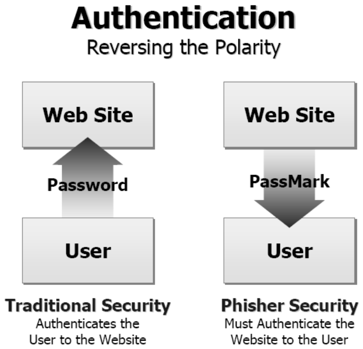

Figure 1: PassMark Security Architecture [17]

In later communications the ID stored in the secure cookie is passed to the server and the selected unique image is sent as part of overall response. However if the user attempts to access the website from a new computer then the associated PassMark is not shown, due to absence of unique device ID. In such cases the user is required to register the unrecognised computer and from then onwards the user PassMark data is displayed.

3 Evaluation and Shortcomings

Microsoft Phishing Filter has a machine learning filter and it uses heuristics to determine if a particular web site looks suspicious or not by looking for characteristics in the page that are common in phishing scams. Since the Phishing Filter heuristics are based on a learning machine, there might be a case where an actual phishing site may not even be flagged as suspicious (false negatives) and some sites which are legitimate could be marked as suspicious (false positive) [18]. Besides the above shortcoming if a new phishing website has not been reported and evaluated by Microsoft then it may remain undetected for sometime.

EarthLink Toolbar visually notifies the user when a site is guaranteed safe, neutral or negative. In essence, the EarthLink Toolbar is similar to MS Phishing Filter. The User Interface of the product needs more work, due to high frequency of warnings and lack of visual representation. Even the sites like PCMag.com are shown in the "neutral" box for no obvious explanation. It is also argued that the frequency with which the shady icon appears during browsing may also quickly numb users to this digital form of crying wolf [19].

By using EarthLink Toolbar the user can also analyse the currently opened web page. The EarthLink system rates the website by gathering information on the owner of the website and the location of the company and/or organization. Along with the rating Company Information, City and Country information is also displayed to the user. EarthLink does not guarantee the results produced as it cannot check for man-in-the-middle attacks, cannot provide correct information if the website is hosted on a third part web server and due to the lack of real-time analysis occasional new phishing sites may remain undetected for sometime [19].

The solution provided by PassMark Security is far superior to EarthLink, but it has its own shortcomings. For example the PassMark system generates unique system ID when the user registers therefore the user is required to register each new computer. This feature opens the architecture to both pharming and man-in-the-middle attacks, as the user PassMark image is not displayed when the user visits the website by using a new computer and the user is required to register again. For registration of the new computer the user is required to provide some personal information e.g. Login Name, in order to get PassMark data. In case of both Pharming and man-in-the-middle attacks the attacker can display rogue website which looks and feels like actual institutional site, get the user Login Name, pass it to the legitimate website and get the user PassMark image which can be then embedded into the rogue website.

Another problem with this solution is that it requires major modifications in organisational business systems in order to incorporate PassMark Security functionality within the organisational web and email interfaces, thus resulting in low adoption.

4 Architecture of the Proposed Solution

The suggested solution uses a custom built browser plugin, which the user downloads from the organisational website, for example from Westpac Official Website, when they register for the first time. The plugin also has a toolbar component that provides a visual feedback to the user after checking for IDN and verifying the legitimacy of the website. A warning message is also displayed in case of pharming or man-in-the-middle attack and a report of an attack is submitted to the organisation. The plugin is designed to maintain the list of valid organisational IP addresses and the list of impostors which is gathered from anti-phishing groups and other user's reports. Both lists are updateable at the runtime by using an encrypted channel with the server. When the plugin detects the organizational website, it requests the user for login details. On the basis of login details the plugin creates an encrypted composite key and a one-time valid token which is sent to the server over the encrypted channel to authenticate the user.

4.1 Protection against Phishing and Pharming

The solution provides three phase check in order to verify the site and to identify phishing, man-in-the-middle and pharming attacks. All three steps are outlined below with their brief description and illustration how they are used to validate the website and detect an attack.

4.1.1 URL and IDN Spoofing Check

In URL spoofing an arbitrary FQDN (Fully Qualified Domain Name) is displayed in the address and status bars, which is different from the actual location of the page. However in IDN spoofing special Unicode characters are embedded in URLs that render in browsers in a way that looks like the original web site address but actually links to a fake web site with a different address e.g. use of '@' in URL like http://www.yahoo.com@youAreHappy.com. The plugin checks for both URL and IDN spoofing upon website request, before the webpage is loaded into the browser window. If spoofing is detected then the user is alerted and asked to manually enter the URL.

4.1.2 IP Address Check

When the user opens a website in the browser, the plugin detects that it is the organisational website. Upon detection the plugin gets the IP address and verifies it from its locally stored IP address lists. If the IP address is found in legitimate IP addresses list then next step is executed else if the IP address is in bad guys IP list then the attack details are submitted to the organisation and user is automatically redirected to legitimate organisational website.

4.1.3 SSL Certificate Validation and Verification

The plugin first checks for URL and IDN spoofing followed by IP address verification of the organisational website. If first two checks are successful and once the webpage is completely loaded in the browser window, the plugin checks, validates and verifies the received SSL certificate from the certificate issuing authority and directly with the server. This step is more relevant in safeguarding the user against pharming and man-in-the-middle attacks rather than phishing attacks. In a pharming attack, the hijacker changes the IP address at DNS and redirects the user to a different website even when they enter correct address. In such cases the hijacked destination will either send an invalid certificate or no certificate at all.

In case of invalid certificate a warning message is displayed to the user by the browser, however if no certificate is received then the browser does not display any warning and the user may not notice that the lock sign is missing. Moreover in case of complex attacks a virus, worm, Trojan or Adware program can be installed on the user computer which can then be used to change the web browser to function differently e.g. to disable SSL certificate warnings. In relation to pharming, in man-in-the-middle attacks the user may get a certificate which could be issued by forged issuer and the browser may not display any warning or error messages.

In order to protect the user against above mentioned situations, the plugin first checks for the existence of the SSL certificate followed by verification and validation of certificate. The plugin first validates the SSL certificate locally by checking issued to, issued by; common name (CN), organisation and organizational unit (OU) field values. If the above certificate field's match to the plugin's internally stored data then the certificate is checked and verified by the issuing authority i.e. trusted certificate authority and by the server directly by using server IP address. This step protects the user from man-in-the-middle attack as in most applications the certificates are verified by only comparing the CN field in the digital certificate received from the server with the server name in the URL which does not ensure complete absence of man-in-the-middle attack.

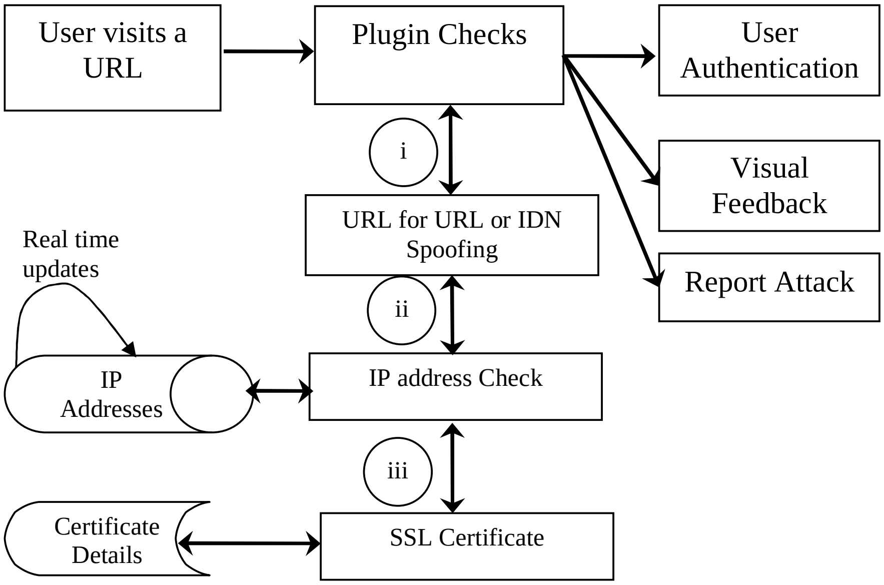

Figure 2: Site Validation and Verification Process

5 Conclusion

In this paper the techniques used to launch phishing, pharming or man-in-the-middle attacks and the available solutions to protect the user from such attacks have been briefly discussed. The architecture of the new site verification technique which safeguards the user against phishing, pharming and man-in-the-middle attacks have been discussed in detail, after analysing the techniques used to launch an attack and the shortcoming of the available solutions. The solution is based on using a custom browser plugin which first checks the requested URL for both URL and IDN spoofing followed by complete site verification which includes IP checks, SSL certificate validation and verification from the trusted certificate authority, directly from the organization server by using server IP address and by locally checking certificate fields. In case of any attack detection, a report is submitted to the server and the user is visually notified. The plugin is still under construction and has not been tested thoroughly to verify its effectives against all possible attacks.

6 References

[1] Faltstrom, P. (March 2003) "Internationalizing Domain Names in Applications (IDNA)", http://www.ietf.org/rfc/rfc3490.txt
[2] Rescorla, E. (May 2000) “HTTP Over TLS”, http://www.ietf.org/rfc/rfc2818.txt
[3] Westpac Banking Corporation, Australia (http://www.westpac.com.au)
[4] Latest Hoax Email Scam Information and Examples on Westpac Bank, Australia, (http://www.westpac.com.au/internet/publish.nsf/Content/PBOB+Latest+virus+information)
[5] Berners-Lee, T (December 1994) “Uniform Resource Locators (URL)” IETF Network Working Group (http://www.w3.org/Addressing/rfc1738.txt)
[6] Fisher, D. (January 2004) “Warn when HTTP URL auth information isn't necessary or when it's provided”. Bugzilla URL (https://bugzilla.mozilla.org/show_bug.cgi?id=232567)
[7] Microsoft (March 2006) “A security update is available that modifies the default behavior of Internet Explorer for handling user information in HTTP and in HTTPS URLs” Microsoft Knowledgebase (http://support.microsoft.com/kb/834489)

[8] Litan, A.(May 2004) "Phishing Victims Likely Will Suffer Identity Theft Fraud", Gartner (http://www.gartner.com)
[9] Phishing Activity Trends Report (January 2006), (http://www.antiphishing.org/reports/apwg_report_jan_2006.pdf)
[10] Anti-phishing White Paper (September 2005) "Microsoft Phishing Filter: A New Approach to Building Trust in E-Commerce Content" URL http://www.microsoft.com/downloads/details.aspx?FamilyId=B4022C66-99BC-4A30-9ECC-8BDEFCF0501D&displaylang=en
[11] Microsoft Phishing Filter Add-in for MSN Search Toolbar, "Dynamic Service Helps Protect Against Fraudulent Websites and Personal Data Theft" URL http://addins.msn.com/phishingfilter/
[12] Internet Explorer 7 Beta 2 Preview, Technology Overview (January 2006), http://www.microsoft.com/downloads/details.aspx?FamilyId=B2AC8F30-2D88-45B6-90AE-ED266161F463&displaylang=en
[13] Microsoft Corporation. (August 2005), "Microsoft Internet Explorer (Pre-Release Version 7.0) Privacy Statement"(http://www.microsoft.com/windowsvista/privacy/ieprivacy_pr7.mspx)
[14] For detailed information on EarthLink Toolbar please visit http://www.earthlink.net/software/free/toolbar/
[15] For detailed information on Mozilla Firefox please visit http://www.mozilla.com/firefox/
[16] http://www.passmarksecurity.com
[17] Security White Paper (2004) "Protecting Your Customers from Phishing Attacks - An Introduction to PassMarks", www.PassMarkSecurity.com
[18] IEBlog. (September 2005), "Phishing Filter in IE7" URL http://blogs.msdn.com/ie/archive/2005/09/09/463204.aspx
[19] Karagiannis, K. (November 2004), “EarthLink Toolbar Review”, PCMag.com http://www.pcmag.com/article2/0,1895,1729638,00.asp