ISSN: 2349-7300
ISO 9001:2008 Certified
International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences
(IJIRMPS)
Volume 1, Issue 2, December 2013

Result Evaluation for Anti-Phishing Design Using Mutual Authentication Technique

M Bargadiya, N Kumar

***Abstract:* Phishing is a type of social engineering attack that aims to gather personal information from a user by delivering an email under the masquerade of a truthful division. Phishing attacks have been growing rapidly and try to damage financial and social aspect at the personal as well as industry altitude. Phishing has primary four different types of impact that are of concern to the personal and financial region. Impacts are Economic Loss, Lack of confidence on Internet, Difficulties in Fraud Investigation.**

In this paper we discuss effectiveness of various anti-Phishing toolbars against phishing attack. In first step we obtain 10 Phishing URL from Phish tank and examine them with five popular Anti-Phishing toolbars. In second step we examine test phishing website with same Anti-Phishing toolbars and our proposed system anti-Phishing design using mutual authentication approach, in last step we summarized the result. Finally we suggest the way to improve the anti-phishing tools with the minimum change in existing security system.

***Key words:* - Phishing, Anti-Phishing toolbar, Vishing, Whaling and Spear Phishing.**

I. INTRODUCTION

In the financial year May 2004-05 it was estimated that $929 million dollars lost to phishing attack [1] [2]. Since then a vast variety of different attacks and techniques have become common, including those highlighted below:

Link Manipulation: One of the most basic attacks was to send users an email with a link to a misspelled or misleading domain, which appear alike to a genuine site. The client is then trap into phishing attack and give there personal or confidential information to phisher.

Social Media: One of the main intentions of phishing movement is public network sites like MySpace and Face book [3]. In 2006 phisher change links on MySpace, and redirect clients to fill login details. The gathering of complete information accumulate on public networking sites formulate them a tempting target for phishing attacks.

Vishing: Phishing attacks were executed against targets outside the web. By with voice over IP (VoIP) expertise, invaders were able to use community confidence in the land-line system by spoofing caller IDs. Programmed communication claim to be from a financial institute were used to gather the information of financial accounts [4].

Spear Phishing and Whaling: Spear Phishing is designed to exploit information disclosed through other means, for example leaked usernames [5]. Whaling is aimed at executive level users, where a single cracked account can lead to major information loss [6].

II. IMPACT OF PHISHING

Phishing has various types of impact, directly as well as indirectly, that are hazardously affect the financial sectors:

Economic Loss. E-commerce businesses may be decries by phishing attack. For example, client generally uses the internet banking for the transaction if he or she trapped in phishing then it directly affects the financial system.

Lack of confidence on Internet. Phishing also weaken the faith in the Internet. By making clients doubtful about the reliability of financial system, and even the online system, phishing can make them less liable to use the Internet for financial communication. [7]. This outlook finds support in a 2005 Consumer Reports survey, which showed declining confidence in the security of the online [8].

Fraud Investigation: Phishing can be performing from any place where phishers can take Internet access. Phisher in one country acquire control of a workstation in another country, and then uses that workstation to host his phishing website or send his phishing e-mails. Such investigations require support between law enforcement agencies in various realms may be necessary for crime investigation.

The Anti-Phishing Work Group (APWG), “Phishing Activity Trends Report 1st Quarter, 2010”.Analyzes quarterly phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization’s website at http://www.antiphishing.org. Number of unique phishing email reports received in March 2010 by APWG from consumers is 30,577. Number of unique phishing web sites detected in March 2010 is 29,879 [9].

III. PROPOSED SYSTEM

In our Anti-Phishing Design Using Mutual Authentication Approach we are assuming that user must present to complete some formalities such as give some welcome messages for the server generated user screen, must submit or select some images, to create random generated graphics password and select questions & give the answers in one word. User must provide personal mobile number for secure one time password receiving agent. After completing the formalities user receives a unique User Identification Number for the initial steps in the login. Finally user selects an alphanumeric password as Final Password with one time password. Now we are presenting proposed authentication steps for the novel method “Anti-Phishing Design Using Mutual Authentication Approach” following steps are:

Step 1 C: [U_ID + Req_S_Auth]
Step 2 S: [Resp_S_ID + U_SD]
Step 3 C: [Resp_U_SD + Req_M_Key]
Step 4 S: [Resp_M_Key + U_SD]
Step 5 C: [M_Key + U_Key]
Step 6 S: [Acknowledge to C]

IV. RESULT ANALYSIS

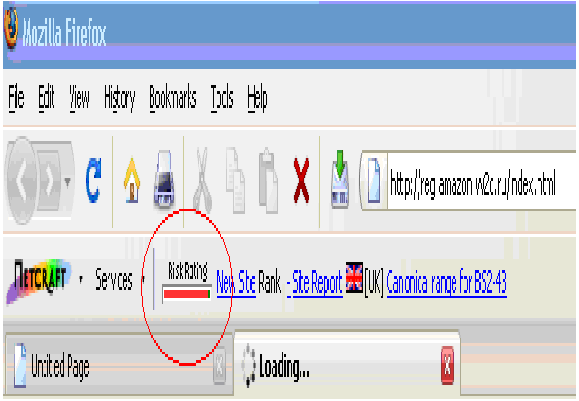
For result analysis, we collect 10- Phishing URL form PhishTank website and check all the phishing URL with Five Anti-Phishing Toolbars and getting response of different tool bars.

Ten Phishing URL form PhishTank [10]:

[1] http://dxyk7.cjb.net/
[2] http://www.gorgl.com
[3] http://www.amazoncomprasbrasil.com.br/
[4] http://reg.amazon.w2c.ru/index.html
[5] http://gmailsecurityverify.tk/
[6] http://www.googlechechkout.com/
[7] http://metalfrost.altervista.org/
[8] http://HSBCupdate.fileave.com/HSBC
[9] http://new.kerckebosch.net/js/update.html
[10] http://www.fuizesbooks.com/update/index9.php

Here we show response of five Anti-Phishing toolbars for phishing URLs:

Netcraft Toolbar response for phishing URL: This requires end users to pay attention to the indictor for each site they visit which is impractical because many users would forget or not realize they should be paying attention to the indicator.

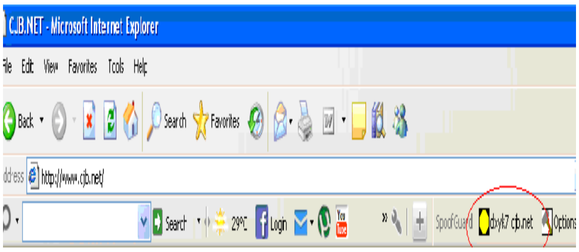

Mozilla Firefox

http://reg.amazon.w2c.r.u/index.html

File Edit View History Bookmarks Tools Help
NETCRAFT
Services
Risk Rating
New Site Rank - Site Report [UK] Canonica range for B52-43
Untitled Page
Loading...

Fig 1: Netcraft response for Phishing URL

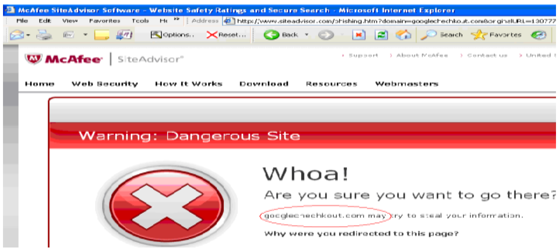
Spoof guard toolbar response for phishing URL: The toolbar primary verifies the present domain name and evaluates it with sites that have been recently visited by the client to identify deceptive web sites that have a similar-looking domain name.


C.B.NET - Microsoft Internet Explorer

Address http://www.cb.net/

Fig 2: Spoof guard response for phishing URL

MacAfee Site Advisor response for phishing URL: Site Advisor can detect phishing websites, website that send spam, spy ware and other malicious things. MacAfee Site Advisor uses the permutation of some heuristics and manual verification.


McAfee SiteAdvisor Software - Website Safety Ratings and Secure Search - Microsoft Internet Explorer

Address http://www.siteadvisor.com/phishing.htm?domain=googlechechkout.com&originalURL=130777

Warning: Dangerous Site

Whoa!

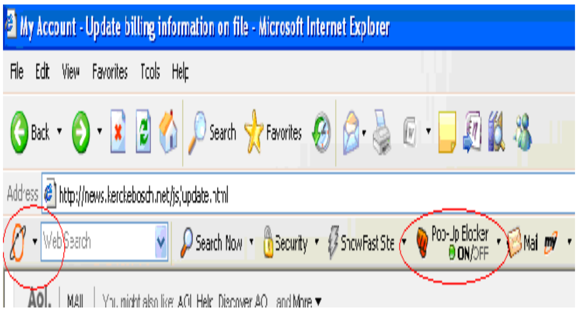
Are you sure you want to go there?

googlechechkout.com may try to steal your information.

Why were you redirected to this page?

Fig 3: MacAfee response for phishing URL

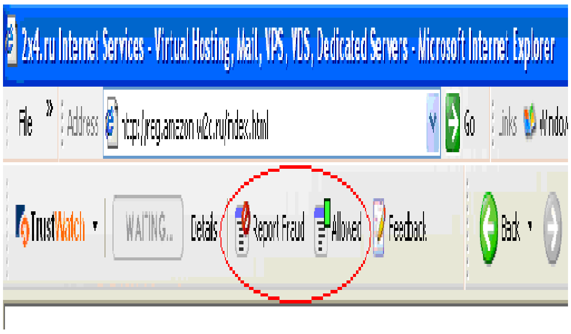
EarthLink Toolbar response for phishing URL: The EarthLink Toolbar work with the combination of client ratings and manual verification. The EarthLink Toolbar permits client to report suspected phishing sites to EarthLink.


My Account - Update billing information on file - Microsoft Internet Explorer

Address http://news.kerckebosch.net/js/update.html

Fig 4: EarthLink response for phishing URL

Trust Watch Toolbar response for phishing URL: GeoTrust Trust Watch toolbar gets its information for phishing site based on particular URL have SSL certificate or not. Generally indicators responses are not found correct in our testing.

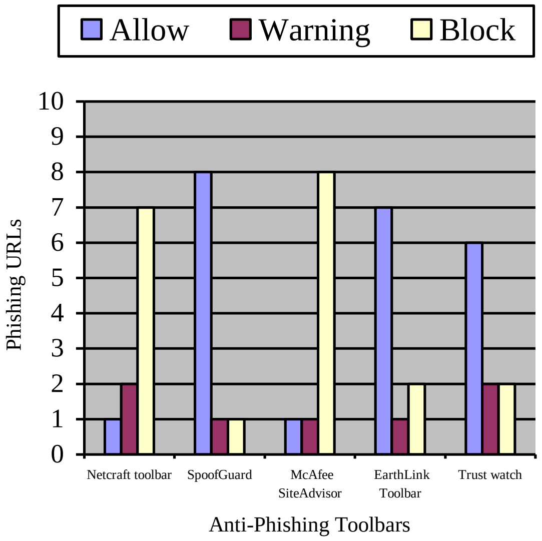


2x4.ru Internet Services - Virtual Hosting, Mail, VPS, VDS, Dedicated Servers - Microsoft Internet Explorer

Address ttp://reg.amazon w2c.ru/index.html

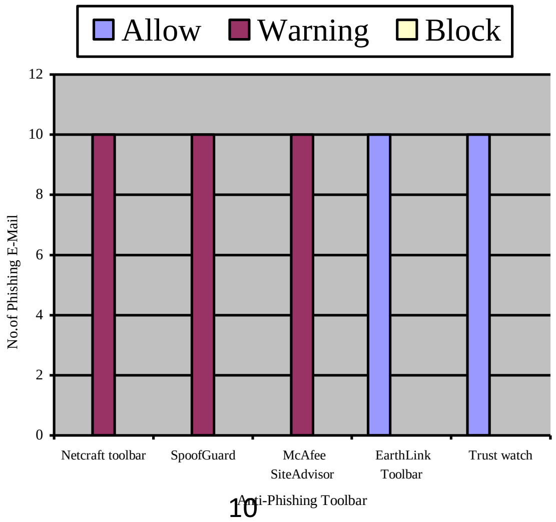
Fig 5: Trust Watch response for phishing URL

Above test shows that all the toolbars are depended on some essential information such as black or white list, diverse heuristics, client ratings and manual verification etc., but toolbar can give limited security against phishing attack.



Graph 1: Response of Anti-phishing Toolbars for phishing URL.

Now we check the Anti-Phishing toolbar against phishing test email which contains map hyperlink and redirect the user to test phishing site. For this purpose we take permission to all the users which are participate in this test. We send phishing mail to 10 users and check the response of different tool bars as

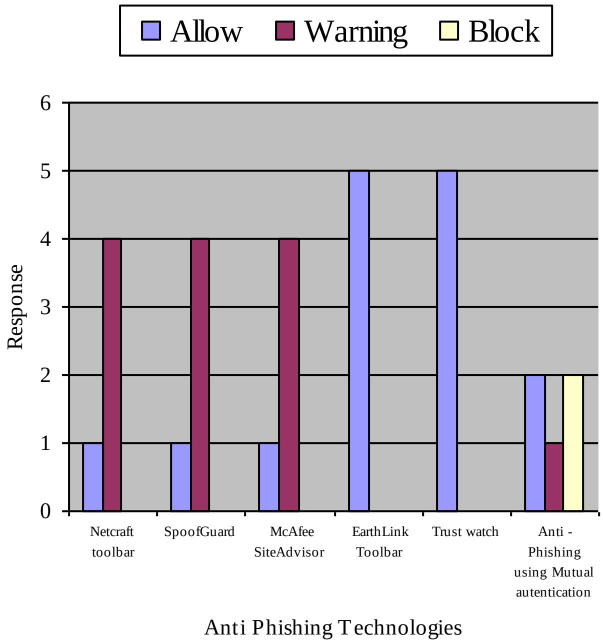


Graph 2: Response of Anti-phishing Toolbars for phishing Email

Now we check the performance of various anti-phishing techniques under phishing attack: For this experiment we design two web sites, one as an original web site and second as a phishing website. Now we test two websites and taking response of anti-Phishing technologies as:

Table 1: anti-phishing techniques performance

Response	Netcraft toolbar	Spoof Guard	McAfee Site Advisor	EarthLink Toolbar	Trust Watch	Anti -Phishing using Mutual authentication
Allow	1	1	1	5	5	2
Warning	4	4	4	0	0	1
Block	0	0	0	0	0	2



Graph 3: Performance of various anti-phishing techniques under phishing attack

V. CONCLUSION

We perform an analysis of the phishing and the line of attack in which it affect the client & association. Anti-Phishing Toolbars are most common and easily available on the web; our study shows that they are good in case of well known phishing web site and URLs but less trustworthy if attack pattern or URL is new. Proposed approach “anti-Phishing design using mutual authentication” is good enough in the case of financial organization.

REFERENCES

[1] "In 2005, Organized Crime Will Back Phishers". IT Management. December 23, 2004. http://itmanagement.earthweb.com/secu/article.php/3451501.

[2] Abad, Christopher (September 2005). "The economy of phishing: A survey of the operations of the phishing market". First Monday. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1272/1192.

[3] Lada A. Adamic and Eytan Adar. Friends and neighbors on the Web. Social Networks, 25(3):211–230, July 2003.

[4] Gonsalves, Antone (April 25, 2006). "Phishers Snare Victims With VoIP". Techweb. http://www.techweb.com/wire/security/186701001.

[5] http://www.microsoft.com/canada/athome/security/email/spear_phishing.mspx.

[6] http://www.theregister.co.uk/2008/04/16/whaling_expedition_continues/.

[7] Stevenson, Robert Louis B. Plugging the "Phishing" Hole: Legislation versus Technology, 2005 Duke Law and Technology Review 0006.

[8] Leap of Faith: Using the Internet despite the Dangers, Consumer Reports Web Watch, October 2005. www.consumerwebwatch.org.

[9] http://www.antiphishing.org.

[10] https://www.phishtank.com/phish_archive.php.