Which web browser work best for detecting phishing

Noman Mazher[1]
Imran Ashraf[2]
Ayesha Altaf
[1]*Department of Information Technology University of Gurjrat, Gujrat Pakistan*
[2]Lecturer Faculty of CS & IT, University of Gujrat, Gujrat Pakistan
[3]Lecturer Faculty of CS & IT, University of Gujrat, Gujrat Pakistan
[1]noman.mazhar@cgc.edu.pk
[2]imranashraf@uog.edu.pk
[3]ayesha.altaf@uog.edu.pk

Abstract:
Phishing is the technique of social engineering in which important information are hijacked. To prevent phishing the easiest way is to blacklist such web sites which are suspicious;, but there are many new phished websites that are not blacklisted. To protect users from those phishing sites many ways are available; one of those is to implement security toolbar in web browser. Now a day every modern web browser has its own implicit security toolbar. Our research is based on the evaluation of toolbars attached with Internet Explorer, Mozilla Firefox and Google Chrome. In our experiment we appraised toolbars attached with these most popular web browsers. Results evaluation showed that Google Chrome provides best security against phishing websites.

Keywords: phishing, security toolbars, web browsers

I. INTRODUCTION

Phishing is the technique of social engineering in which important information of user such as credit card, email password etc are hijacked.

According to APWG survey in the last month of 2012 45,628 phishing websites have been detected [1].According to AWPG report 34.4 % financial websites, 32.1 % payment sites, 14.7 % gaming sites , 6 % social networking sites has been detected as phishing sites in the last quarter of 2012 .

To prevent users from phishing attacks from these websites there can be two approaches; one is to blacklist phished websites. In this method URL of each website is checked in phishing detection engines like phish tank etc [2]. But this will not completely protect against phishing website because there are many newly created web sites which are not in this pool. Second approach is called heuristic-based approach. In this approach it is tried to detect phished pages on based on some factors such as checking its URL authenticity etc [3]. Content of web pages can also be used for phishing detection [4]. There are also some approaches based on machine learning for the same purpose [5], [6]. Some artificial intelligent systems [7] [8] have also been introduced for detection phished pages. One other such technique is the use of security toolbars [9]. Our research will focus on detecting phished pages using web browser's security toolbars that are an internal and essential part of each advance web browser. We will focus on three popular browsers; Internet Explorer, Mozilla Firefox and Goggle chrome. The main focus is to evaluate the performance comparison of security toolbars of the mentioned browsers. The next section describes the use of security toolbar to detect phishing. .

II. BACKGROUND

As our main focus is on web browsers security system, for experiment we are taking three most popular web browsers; Internet Explorer, Mozilla Firefox and Google chrome. Before analyzing their security model we will describe the factors involved in security [10].

Certificate:

There are some standard security authorities that give each web page a specific identity that is called digital signature which is intact binding of public key with an identity. It is also possible for a company to give its own certificate rather than any security authority. Web browser gives warning and gives user an option to either accept that certificate or not.

HTTPS:

HTTP stands for hyper text transfer protocol. HTTPS is the extension of HTTP. HTTPS is a secure HTTP protocol which describes that either that web page is sent through SSL/TSL or not.

SSL:

SSL stands for Secure Socket Layer. This is a cryptographic protocol. SSL is used for authentication purposes.

TSL:

TSL stands for Transport Security Layer. TLS is used for secure communication over the server [10]. Purpose of these protocols is to ensure authenticity and security.

978-1-4799-2622-0/13/$31.00 ©2013 IEEE

After describing some security terms now we will focus on web browsers security warning that they use in case of finding suspicious web site .

WEB BROWSERS SECURITY MODEL

Here are the chosen popular web browsers and their security models.

Internet Explorer:

Internet Explorer is one of the most popular and most mature web browsers. This is a product of Microsoft Corporation. Microsoft has its own security and safety center [11, 12]. Internet Explorer 10 helps user in security by following actions.

Fig 1. Warning system of IE 10

It gives a warning message if user wants to download any content which is not commonly downloaded

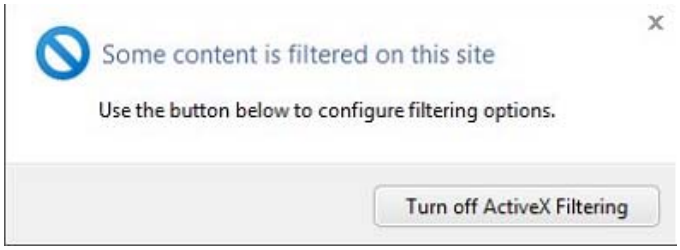

Fig 2: Filtered content security on IE 10

IE allows user to filter the websites which should run ActiveX control and which should not.

Mozilla Firefox:

Mozilla Firefox is also one of most popular open source web browser. It also has its own security center, which provides user many tips for assuring their security [13]

Fig 3 : Firefox security against suspicious page.

Here is an example of security model of Firefox .If Mozilla Firefox gets suspicious page it bocks that page...

Google Chrome:

Google Chrome is one of fastest growing web browser which is introduced by Google Corporation. Google choom has also introduced security feature against suspicious web pages [14]

Fig 4: Google chrome security warning

Google chrome introduces safe browsing technology that displays security warning page in case of suspicious URL. This feature is specifically introduced for prevention of phishing attacks.

In this section we introduced some security terms and security feature of popular web browsers. In next section we will describe our experiment. This experiment will prove that these security features are not enough to provide security against phishing.

2. EXPERIMENT

Study Design:

To observe efficiency of web browsers against phishing we conduct an experiment. As discussed earlier we have targeted three web browsers; Mozilla Firefox, IE 7 or above and Google Chrome. For target audience we choose student of information technology because these students can be assumed most literate about web surfing rather than students of other fields .and for website to be phished we choose most popular social networking website [14] face book. Other website that we choose for phishing is Gmail because they have their official email ids are on Gmail.

Fig 5: phished face book page

Scenario and Procedure

In our experiment we develop pages which are visually similar to original web sites. We upload these pages on free hosting site. After preparing that all we asked student to go to specified URL, which was www.myfb.comze.com Participants are given following scenario "Imagine that you receive an email message that asks you to click on one of the following links" [10]. And one restriction was to use only from one of above three web browsers. After entering address on their browsers they have to report what happened in case of each web browser.

Tools and Technology used:

Phishing page was designed using HTML as front end language and php as server side scripting language. These pages were hosted on 000webhost.com. Domain name chosen for the experiment was "myfb.comze.com"

Participants Demographic:

In conducted experiment, we took the help of 46 participants. These participants were chosen on an assumption that they know how to use computer, web and email and were all regular users of face book and Gmail.

Sex:

48 % of the participants were female (22 participants) and 52 % were male (23 participants).

Age:

Age of participants ranged from 18 to 35 years; from which 54.3 % were between 18 to 20 years. 15.3 % between 20 to 25 years and 3 % between 25 to 35 years.

OS:

As a primary operating system 2.2 % participant used Mac OS, 17.8 % participants used Windows 8 and 80 % participants used windows 7.

Hours using computer

Hours of computer used ranges from 10 to 135 hours average .

III. EXPERIEMENTAL RESULT

Evaluation Criteria

For evaluation of our experiment we decided evaluation criteria which are mostly used for comparing classifier. According to criteria following metrics are used for testing our results [18].

True Positive (TP): the number of phishing pages detected as phished pages.

True Negative (TN): the number of phished pages that were assumed legitimate pages.

False Positive (FP): the number of legitimate pages which were classified phishing pages.

True Positive Rate (TPR):

It is also called hit ratio. This is ratio which is calculated by dividing pages detected as a phished pages by total phished pages in test data. This is calculated by.

TPR = ∑ phishing detected / ∑ phishing site in test data

False Positive Rate:

It is number of legitimate websites that were wrongly detected as phished site divided by total number of legitimate site in test data

FPR = ∑ legitimate detected / ∑ legitimate site in test data

Performance Evaluation:

In our experiment we observed that our participants that used IE were easily phished as they did not get any alarm by their browser. Almost same was the case with Mozilla Firefox. But Google Chrome users got a warning page when they hit on that phished URL. So TPR was very high in Google chrome rather than TPR in IE and Mozilla Firefox.

Results of our experiment are plotted in the graph below

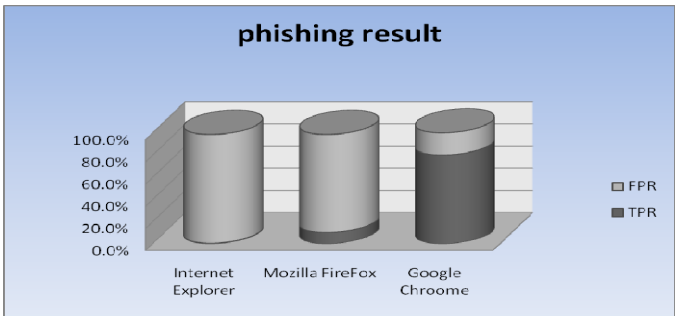

Fig6 : Result of our experimentaph

	Internet Explorer	Mozilla FireFox	Google Chroome
TPR	0.5%	10.0%	80.0%
FPR	98.0%	88.5%	20.0%

Fig 7: classification performance

Our results show that from the selected browsers Google chrome presents the best security to detect the legitimate or phished pages.

IV. CONSLUSION AND FEATURE WORK

In our research we evaluated a dimension of detecting phishing websites, and that dimension is about web browser's security toolbars. After phishing experiment we found that Google chrome provides best security against phishing than other web browsers. But Google chrome still does not provide total fool proof security.

Although it provides a warning screen in case of any suspicious URL, yet it allows users to "proceed at their own risk. So it is still on user end that either he/she follows its instructions and stop surfing further or proceed further. Secondly there are some web pages that are legitimate but it also give warning for those pages i.e. it just check URL which is not enough.

Our study was just about case of phishing scam where any URL is sent to users for phishing. We do not cover other case of phishing where URL spoofing is also used. In those cases Google chrome is not able to find it as a phishing site and does not provide warning screen to users. For further research we intend to use other phishing techniques. Experiment includes URL spoofing and visual similarity based phishing detection of these web browsers.

References

[1] S. b. Baunfire.com, "Unifying the Global Response to Cybercrime | APWG," 2013.

[2] (2013). *PhishTank | Join the fight against phishing*. Available: http://www.phishtank.com/

[3] I. Jo, E. Jung, and H. Y. Yeom, "You're Not Who You Claim to Be: Website Identity Check for Phishing Detection," in *Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference on*, 2010, pp. 1-6.

[4] K.-T. Chen, J.-Y. Chen, C.-R. Huang, and C.-S. Chen, "Fighting phishing with discriminative keypoint features," *Internet Computing, IEEE,* vol. 13, pp. 56-63, 2009.

[5] N. Sanglerdsinlapachai and A. Rungsawang, "Using domain top-page similarity feature in machine learning-based web phishing detection," in *Knowledge Discovery and Data Mining, 2010. WKDD'10. Third International Conference on*, 2010, pp. 187-190.

[6] D. Miyamoto, H. Hazeyama, and Y. Kadobayashi, "An evaluation of machine learning-based methods for detection of phishing sites," in *Advances in Neuro-Information Processing*, ed: Springer, 2009, pp. 539-546.

[7] P. S. Andrews and J. Timmis, "On diversity and artificial immune systems: Incorporating a diversity operator into aiNet," in *Neural Nets*, ed: Springer, 2006, pp. 293-306.

[8] X. Fang, N. Koceja, J. Zhan, G. Dozier, and D. Dipankar, "An artificial immune system for phishing detection," in *Evolutionary Computation (CEC), 2012 IEEE Congress on*, 2012, pp. 1-7.

[9] M. Wu, R. C. Miller, and S. L. Garfinkel, "Do security toolbars actually prevent phishing attacks?," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 2006, pp. 601-610.

[10] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 2006, pp. 581-590.

[11] (2013). *Microsoft Word - Kajiyama_Takahiko_with_Comments2 - Kajiyama_Takahiko.pdf.* Available: http://sdsu-dspace.calstate.edu/bitstream/handle/10211.10/3522/Kajiyama_Takahiko.pdf?sequence=1

[12] C. Almond, "A practical guide to cloud computing security," *A white paper from Accenture and Microsoft,* 2009.

[13] R. Dhamija and J. D. Tygar, "The battle against phishing: Dynamic security skins," in *Proceedings of the 2005 symposium on Usable privacy and security*, 2005, pp. 77-88.

[14] C. Reis, A. Barth, and C. Pizano, "Browser security: lessons from Google Chrome," *Queue,* vol. 7, p. 3, 2009.