Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 100 (2016) 43375-43378

ISSN: 2229-712X

Detection of Online Phishing Attacks Using a Transparent Proxy System

Akinlolu, A.O[1] and Jimoh, R.G[2]

[1] ICT Unit, Fountain University, Osogbo, Osun, Nigeria

[2] Department of Computer Science, University of Ilorin, Ilorin, Kwara, Nigeria.

ARTICLE INFO

Article history:

Received: 23 June 2016;

Received in revised form:

26 October 2016;

Accepted: 01 November 2016;

Keywords

Phishing, proxy,

Countermeasures,

Detection,

Transparent.

ABSTRACT

The Internet has increasingly become a valuable tool. Despite the benefit, the Internet can often represent an insecure channel for exchange of information. Among the challenges that have now affected the Internet users is phishing. This study propose a secure Anti-Phishing system using a Transparent Proxy System. The proposed system is a middleware that is located between the clients and a content provider. The proposed system was able to detects, alerts novice and experienced users of potential phishing threat.

Introduction

The Internet revolution has had impacts in almost every area of human endeavor. From individual, business, industry, government to not-for-profit organizations, Internet has simplified, speeded up, and even revolutionized communications [10]. Over the past twenty years, the Internet has radically transformed the way people communicate, both locally and globally [5].

Despite the benefit, the Internet can often represent an insecure channel for exchange of information leading to a high risk of intrusion and fraud [8].

As one of the top cybercrime tactics impacting both consumers and businesses, phishing has remained a consistent potent threat over the past several years [3].

Widely known today, the first instances of phishing attacks occurred in the mid 1990's and targeted America Online (AOL). The attackers typically used either instant messages or email to trick users into disclosing their AOL passwords. Victims would provide the attackers with this information, which the attackers would later leverage to assume ownership of the victim's AOL account. The account could then, for example, be used to send Spam and the like [6].

The term phishing comes from the analogy that Internet scammers are using e-mail traps to fish for passwords and financial data from the sea of Internet users' data [1]. Apparently, the "ph" was used as a tribute to the term "phone phreaking", a technique used in the early days of hacking to have advantage of security weaknesses in the phone systems. Phishing is defined as the use of spoofed emails and deceitful web sites for the purpose of fooling users into revealing personal data [1].

Phishing attacks are becoming increasingly pervasive and sophisticated [2]. Phishing has spread beyond email to now comprise of VOIP, SMS, instant messaging, social networking sites, and even massively multiplayer games [2].

Criminals are also shifting from sending out mass emails in the hopes of tricking anyone, to more selective spear-phishing attacks which use relevant background information to trick specific victim [2].

Efforts have been made in various studies by adopting Genetic Algorithm, Fuzzy Logic and Data Mining Algorithm to detect and prevent phishing [9]. The Fuzzy Logic and Data Mining Algorithm approach which initially assesses system and classifies phishing emails based on their contents. After the email has been assessed and classified, the system effectively gets rid of the Phishing site or Phishing page by sending a notification to the System Administrator of the host server i.e. hosting a Phishing site which may result in the removal of the site [9].

In addition, a related approach using the computer systems application firewalls to protect users from the deceit cases with URL filtering and anomaly detection [4]. In this research work, thwarting of phishing attack was done by applying simple algorithm into an open source Privoxy system [4]. The proxy system was unable to serve as a transparent proxy server where Internet users' browser settings affect the operations of the designed anti-phishing system. Also, to enable the proxy system work distributedly, that is, on a large number of computer systems, the designed proxy system is needed to be installed on all users systems.

The anti-phishing system proposed by Miyamoto et al. (2005) would have been more efficient if the simple filtering algorithm was implemented on a transparent proxy server. By doing this, it will allow large number of computer systems to be connected without prior installation of the SPS. In addition, by designing the anti-phishing system to allow automatic updates of rule set, URL blacklist and whitelist will improve the performance of the anti-phishing system.

This research aim is to propose a secured Anti-Phishing system using a Transparent Proxy System to reduce the internet innovation setback which comes with it associated

Tele: 2348050313501

E-mail address: akinlolu.azeez@gmail.com

challenges i.e insecurity of information across the network (R. G. Jimoh, Personal communication, June 2015).

The associated challenges experienced from the use of Internet today despite its benefits [4] is the motivation behind this research work and for the reason that phishing is well known, still it poses a significant security threat to the society where a large number of Internet users fall victims to the fraud, causing loss of billions of naira forms the gap in this area of research. In view of this, the researcher is willing to implement phishing detection and update script into an open-source proxy which will be called a Transparent Proxy System to detect online phishing attacks will go a long way in safeguarding our online transaction activities.

Transparent Proxy System

The proposed Transparent Proxy System (TPS) will be a middleware that is located between the clients (Internet users) and a content provider (server) which will filters messages passing through them. The aim of the TPS is to intercepts the requests made by the Internet users and perform various operations such as caching, URL matching, filtering, and authentication then passes the outcome to the destination (Internet). It receives and reverses the reply from the destination server to the requesting clients' browsers.

Algorithm: TPS main routine

```
1: procedure TPS_PROXY main routine
2: for all httpRequest from client do
3:     send httpRequest to Squid
4:     receive httpResponse from Squid
5:     if URL != VALID URL then
6:     send error page to client
7:     else
8:     apply DANSGAURDIAN PROXY to httpResponse
9: send httpResponse to client
10: end if
11: end for
```

Figure 1: Transparent Proxy System Main Routine.

The researcher implements TPS based on an open source proxy called Squid and Dansguardian. Squid which responses to all HTTP requests is expected to send back an error page message if a URL is invalid or its host is unavailable. Valid websites / URLs are later handled by the Dansguardian system.

The Dansguardian proxy system was applied with automatic ruleset update script, setup to detect anomalous URL, web links which belongs to the online Phisher. It provides an alert page for the Internet users, notifying users that the visited website content has a phishing property which has matched the ruleset provided in the Transparent Proxy System.

A proxy server system that integrates both Squid and Dansguardian web content filtering was created for an anti-phishing operation. The researcher configures squid to work as a transparent proxy which receives all redirected outgoing web and HTTP request made by anyone other than TPS by the Squid listening port (port 3128). Squid proxy sends HTTP request to Dansguardian system which performs HTTP rule-set match and phishing attacks response.

For the Transparent Proxy System to function as an efficient anti-phishing solution, it is required to be implemented on a computer system which has a Linux based operating system. The Transparent Proxy System resides in the server system. This is necessary in order to connect clients systems transparently where connected Internet users require no configurations nor setup their Internet browsers before the TPS initializes their computer systems.

Moreover, a script was implemented with the Dansguardian system which does the automatic updates of the rule set contained in the Dansguardian proxy. By doing this, the TPS was used with convenience by the end users so therefore they won't have to manually populate the white-list and blacklist with newly reported phishing website which will now be done automatically as at when due.

Algorithm : AUTOMATIC TPS UPDATE

```
1: Start
2: "Procedure for Automatic_TPS_Update"
3: For all List Update request from admin do
4:If (UPDATE == AVAILABLE) Then
5:Gain TPS root privilege
6: access DANSGUARDIAN directory
7: Delete phishing.tar.gz
8: Add new phishing.tar.gz
9: Unzip phishing.tar.gz
10: Save Script name
11: Make script executable
12: Let script run daily
13: Restart DANSGUARDIAN
14: Else
15: Print "Don't do update"
16: End if
17: End for
18: Stop
```

Figure 2: Automatic Phishing Update Algorithm.

Findings and Results

After all modules of the Transparent Proxy System had been installed and setup, the Internet server system was able to perform it anti-phishing operations. Internet users successfully connect through the TPS filtered network via LAN or wireless access points, TPS automatically initialize the clients system, detect and alert users whenever a malicious website is accessed on the browsers.

Whenever a user makes effort to lunch a URL through the client's browser, the Dansguardian filtering system matches the website against the list of domain and URL in its database. If a website or domain matches, the TPS blocks and denies the website, sends an error page to the Internet users that he or she could not visit the website because it has been flag as a phishing website.

A computer system was connected to the TPS filtered Internet router which was used to surf the web, the Internet user visits some of the listed illegitimate websites in Table 1 and the TPS detects and blocked the visited websites as a phishing page content. The screen-shot of the detected attack is shown in Figures 3.

TABLE 1. List of Phishing Website.

S/N	WEBSITE URL
1	http://paypal.services-limited.cf/
2	http://confirmation-identity.ab.ma/
3	http://kwe2342fsd.rt546sdf234re.com/
4	http://www.theologe.de/
5	http://interswitch001.justfree.com

TPS Update

As described in the design of the TPS, an automatic update of the anti-phishing database was set to perform weekly. The system hosting the TPS was observed after a week to perform its update task. Figure 4 shows the screenshot

of the implemented update script for the automatic database update process.

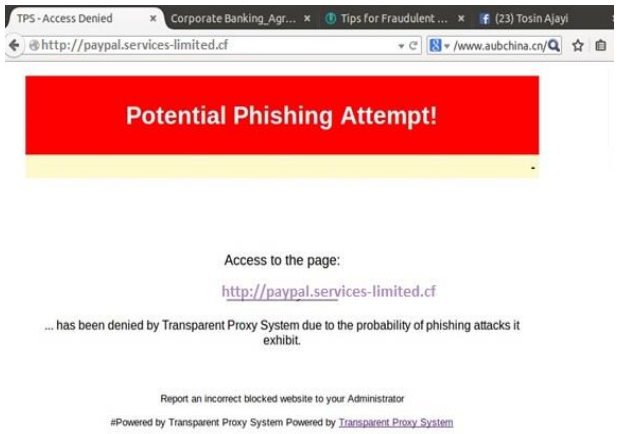


Figure 3: Potential Phishing Attempt Detected by TPS.

update file

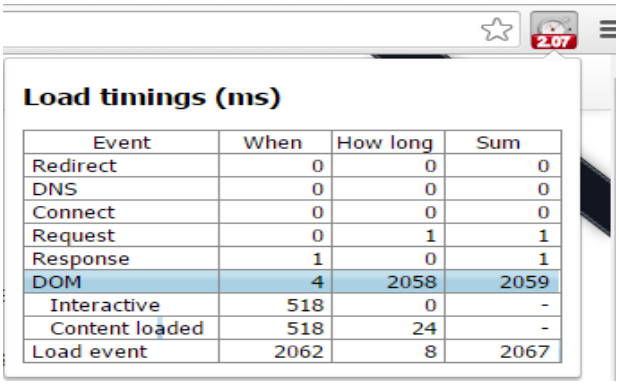
```
1 # blacklists update script for dansguardian
2 cd /etc/dansguardian
3 sudo rm -f phishing.tar.gz
4 sudo rm -rf phishing
5 sudo wget -qnv ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard_contrib/phishing.tar.gz
6 sudo tar -zxf phishing.tar.gz
7 sudo chown -R root.root phishing
8 sudo chmod -R 640 phishing
9 sudo find phishing -name new\* -exec rm {} \;
10 sudo rm -f phishing/usage
11 sudo chmod ug+x phishing
12 chmod +x dansguardian
13 service cron.d restart
```

Figure 4: TPS Database Update Script.

HTTP Content Cache

A static web page sometimes called a flat page or stationary page is a webpage that is delivered to the user precisely as stored, in contrast to dynamic web pages which are initiated by a web application [11]. When multiple Internet users request and visit the same static website frequently, the TPS automatically cache the content of these websites so that the subsequent requests of these same web pages can be displayed in a lesser time.

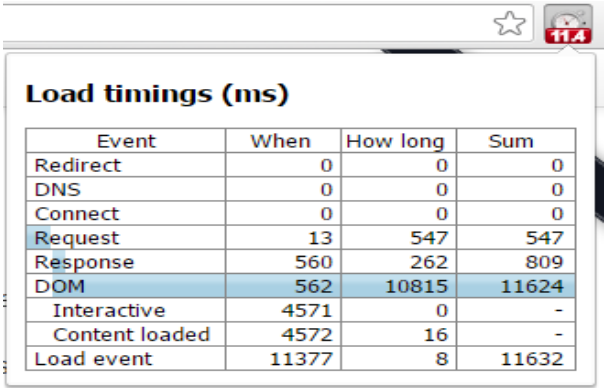
In figure 5, the URL of the website "www.jbake.org" was visited and the client's system requesting the page took **2.07s** response time before the full page of the website could be opened**.**



Event	When	How long	Sum
Redirect	0	0	0
DNS	0	0	0
Connect	0	0	0
Request	0	1	1
Response	1	0	1
DOM	4	2058	2059
Interactive	518	0	-
Content loaded	518	24	-
Load event	2062	8	2067

Figure 5.Cache of Webpage with TPS Internet.

In figure 6, the same URL was visited by another user who is connected to the internet outside the TPS host and it took **11.4s** for the user's browser to fully open the visited website.



Event	When	How long	Sum
Redirect	0	0	0
DNS	0	0	0
Connect	0	0	0
Request	13	547	547
Response	560	262	809
DOM	562	10815	11624
Interactive	4571	0	-
Content loaded	4572	16	-
Load event	11377	8	11632

Figure 6: Cache of Webpage without TPS Internet.

The researcher verifies that the Transparent Proxy System developed for detecting online phishing attacks meets the design requirements. Various operating system environments shown in Table 2 was prepared to test some phishing and emulated legitimate website. Legitimate web pages of enterprises such as Banks, Online payments portal and Online shops were noted to have security lock and secured HTTPS protocol on its URL and experienced Internet users could distinguish between the phishing and legitimate websites**.**

TABLE 2: OS Environment Used for Evaluation.

S/N	OS ENVIRONMENTS	WEBSITES
1	Ubuntu 14.04	http://interswitch001.justfree.com/mukoro/update2009.htm
2	Windows 10	http://confirmation-identity.ab.ma/
3	Mac OS	http://kwe2342fsd.rt546sdf234re.com/
4	Android 4.2	http://paypal.services-limited.cf/
5	Blackberry	http://www.theologe.de/

TPS could identify the phishing sites, blocked all suspicious URL, and alerted its presence to the test users in all system environments in Table 2.

Clients' system environments that were used to test the proposed anti-phishing system for better evaluation were up to 5 including Android OS which is one of the most used mobile operating systems with a large market share [7].

Measurement of Processing Overhead

The researcher evaluates the processing overhead of TPS. The processing overhead is generated by the Internet server system when the TPS checks URLs and phrase match phishing content of the visited web pages. Also, the processing overhead is an important index, because novice users will not satisfied as long as the processing overhead is too big. To evaluate processing overhead, we measure the time spent to open the page content of various website for example www.unilorin.edu.ng in this case and compare the response speed with and without TPS.

Average load times (seconds) for 5 run(s)

Test #	Time	DOM Interactive	DOM Complete	Load Event End
1	11:24:42	3.318	4.568	4.575
2	11:24:48	2.698	3.853	3.859
3	11:24:52	2.7	3.91	3.917
4	11:24:57	3.141	4.119	4.124
5	11:25:03	2.569	3.588	3.596
	Average	2.885	4.008	4.014

Figure 7. Response time on TPS.

Figure 7 represents the load timing of the webpage www.unilorin.edu.ng after the website has been loaded for 5 runs. The average time taken for the whole page to open successfully is **4.01 seconds**.

Average load times (seconds) for 5 run(s)

Test #	Time	DOM Interactive	DOM Complete	Load Event End
1	10:44:06	5.003	24.239	24.255
2	10:44:31	4.941	16.453	16.463
3	10:44:49	4.591	13.242	13.256
4	10:45:03	4.16	10.785	10.793
5	10:45:15	3.667	13.663	13.673
	Average	**4.472**	**15.676**	**15.688**

Figure 8. Web Response time without TPS.

While figure 8 represents the load timing of the webpage www.unilorin.edu.ng on the computer system which does not receives Internet link from the TPS and the total average time taken for the whole page to open successfully is **15.69 seconds**.

From the both run tests, the proposed system took a lesser time to responds to users HTTP requests despite the anti-phishing operations it performs before users request page could be accessible.

Conclusion

Knowing that phishing is a security trend that will only continue, Internet users should adapt safety measures when performing online transactions. Personal information, credentials should not be updated online when requested, only physically when visiting the enterprises office such as Banks, Shops and others. Bookmarking of trusted websites is advised so users can always visit such websites through the browser's bookmark link. Moreover, users who have fall victim of Phishing attacks should endeavour to report such website to Google Safe Browsing team. By doing so, it will help us keep the web safe.

Recommendation

In near future, future researcher should consider an enhanced analysis of attackers' webpages that will help in identifying the closest matches of potential phishing threat possibility without requiring an illegitimate websites to match against the users' web requests.

A content based feature to increases collected phishing ruleset which its believe will be a potential research direction since it helps in understanding the behaviour of the phishing website and could possibly improve the performance of this method.

References

[1] Gerald, G. G., Tan, N. L., & Goh, C. Y. (2008). Phishing; A growing challenge for Internet banking providers in Malaysia. *Communications of the IBIMA*, 133-142.

[2] Hong, J. (2012). The Current State of Phishing Attacks. Communications of the ACM. 55(1), 74-81. New York, NY.

[3] Lungu, I., & Tăbuşcă, A. (2010). Optimizing Anti-Phishing Solutions Based on User Awareness, Education and the Use of the Latest Web Security Solutions. *InformaticaEconomică*, 27-35.

[4] Miyamoto, D., Hazeyama, H., & Kadobayashi, Y. (2005). SPS: A Simple Filtering Algorithm to Thwart Phishing Attacks. In *Technologies for Advanced Heterogeneous Networks* (Vol. 3837, pp. 195-209). Springer Berlin Heidelberg.

[5] Naomi, S. (2013). Language of the Internet. *American University Press*.

[6] Nick, N., Lisa, K.-P., Sonny, A., & Tracey, A. T. (2010). Cybercrime and Business: How to not get caught by the Online Phisherman. *Journal of International Commercial Law and Technology, 5*(4).

[7] Saurabh, B., Priyanka, C., & Preeti, S. R. (2013, February). Android Operating Systems. *International Journal of Engineering Technology & Management Research, 1*(1), 147-150.

[8] Soujanya, K., & Vishnu, V. S. (2015). Enhanced User Security Using Graphical Passwords. *International Journal & Magazine of Engineering, Technology, Management and Research, 2*(8), 1001 – 1009.

[9] Steve, S., Mandy, H., Kumaraguru, P., & Cranor, L. &. (2012). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *Carnegie*

[10] Wada, F., & Odulaja, G. (2012). Assessing Cybercrime and its Impact on E-Banking in Nigeria Using Social Theories. *African Journal of Computing & ICT*, 69-82.

[11] Wikipedia Corporation. (n.d.). Retrieved April 4, 2016, from Static web page: https://en.wikipedia.org/wiki/Static_web_page.