http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (1): 198-203, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.198.203

An Active Anti-phishing Solution Based on Semi-fragile Watermark

Huajun Huang, Yaojun Wang, Lili Xie and Liqing Jiang
College of Computer and Information Engineering,
Central South University of Forestry and Technology, Changsha, 410004, China

Abstract: Although anti-phishing solutions were highly publicized, phishing has been still an important serious problem. One of the main reasons was that phishers cost little to change their targets by copying and then to modify a legitimate site's web pages. In this study, a novel active anti-phishing solution based on semi-fragile watermark was proposed to protect online service provider. Firstly, the semi-fragile watermark was consisted of URL, website identity characters and singular heuristics occurred in phishing attack and actively embedded into the webpage tag by the provider. As a suspicious website was met, the inconsistence of the generated semi-fragile watermark and the extracted information indicated the phishing attack. Simulating phishing experiments shown the solution could effectively thwart the phishing attack by downloading the tactic's webpage and modifying a little to lure the victims.

Key words: Identity theft, phishing, anti-phishing, semi-fragile watermark, equal tag

INTRODUCTION

Phishing, a term coined in 1996, was a form of online identity theft (APWG, 2007). A phishing attack today typically employed generalized "lures." For example, a phisher disguised himself as a large banking corporation or popular on-line auction site by replicating of target web sites. However, over the decade the definition of phishing has expanded. Phishers today use attack vectors such as email, Trojan horse key loggers and man-in-the-middle attacks to trick the victims (Hong, 2012).

Phishing activity is naive but the caused damage is tremendous. According to recent security reports of CNERT/CC in China, 45 million adults lost a total of 7.6 billion RMB directly due to phishing in 2009 (CNERT/CC, 2010). But the damage caused by phishing does not only apply to monetary property alone. Indirect losses were much higher, including of loss of productivity, cost of maintaining a help desk to field calls, recovery costs or damage to an online organization's reputation. This in turn caused a significant loss in money, resources and time (Khatibi *et al*., 2006; Sudha *et al*., 2007).

Another phenomenon was that only small set of targeted sites were imitated by phishers. In order to exploit the financial profit, phishers usually selected famous online e-commerce websites. For instance, August 2011 saw the total number of unique phishing submitted to APAC in China is 3,579. Four brands, such as Taobao, Tencent, ICBC and CCB, hijacked by phishing campaigns and comprised 96.29% of the volume (APAC, 2011).

Quite a number of solutions to mitigate phishing attacks have been proposed to date. Generally, past works could be classified into browser-side-based solution and server-side-based solution (Huang *et al*., 2012). Browser-side-based solution usually embedded anti-phishing measures 'plug-in' into end-user's browsers. Taking the advantage of heuristics (Xiang *et al*., 2011), visual similarity (Chen *et al*., 2010), identity (He *et al*., 2011) and machine learning (Abbasi *et al*., 2010; Zhang *et al*., 2011), the measures could automatically detect phishing sites and warned the end-user to go away from phishing trick. However, it was entirely passive; its effectiveness hinged on users' ability. As we all know, end-users would also be ill-equipped to identify phishing attacks.

An alternative that has been widely adopted was server-side-based solution, which referred to require online organization authentication to defend against phishing attacks. Typical approach attempted to eliminate the phishing problem at the server side by trying to prevent phishing from reaching the potential victims. Industry relied heavily on manually-verified URL black-lists in combating phish. Another authentication approach was to share a secret between server and end-user, e.g., an image watermark (Topkara *et al*., 2005; Huang *et al*., 2010; Singh *et al*., 2011), a fingerprint (Steel and Lu, 2008). However, email filter and black-list verification would unavoidably cause false positive and false negative and secret share required user awareness and prior knowledge.

Corresponding Author: Huajun Huang, College of Computer and Information Engineering,
Central South University of Forestry and Technology, Changsha, 410004, China

The traditional, passive solutions-providing users with tools to make decisions-may not be sufficient. In this paper, an active anti-phishing solution was done by online service provider to protect end-users from making mistakes. The semi-fragile watermark was consisted of URL, website identity characters and singular heuristics. After the embedded semi-fragile watermark into webpage, the online organization could detect replicated phishing sites. Simulating experiments shown the solution could effectively thwart the phishing attack.

WEBPAGE INFORMATION HIDING ALGORITHM BASED ON EQUAL TAG

Webpage information hiding algorithm based on equal tag was proposed by Sun *et al*. (2007) abbreviated in ET lately. The key idea was that tag attributes of webpage may appear in any order. So the order of attributes could be changed, without changing the show or the file length. The tags with different attributes permutation were called equal tag in this study in the following format.

Definition 1: Let $T(a_1, a_2, \ldots, a_n)$ be a tag in HTML, which has n attributes. Where T represents the tag name, a_i has the form "attribute name = value", denotes an attribute in a tag ($1 \le i \le n$).

Definition 2: Let permutation $(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n)$ is a new permutation of $T(a_1, a_2, \ldots, a_n)$, so the tag $T(a_1, a_2, \ldots, a_n)$ is an equal tag of $T(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n)$ and $T(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n) \Leftrightarrow T(a_1, a_2, \ldots, a_n)$.

A cover-webpage is modified by equal tag had the same show on the browser. So, there have some properties of equal tag:

- **Property 1:** Equal tag has the same function
- **Property 2:** $T(a_1, a_2, \ldots, a_n)$ has n! equal tags

Semi-fragile watermark is new tendency to watermark. The semi-fragile watermark must fit to the following two conditions:

- It is robust to the provider normal operation, such as updating the news, advertisement and so on
- It is fragile to the phisher malicious operation, such as changing the host name of server form handler, the title and so on. The phisher activity in reality is shown in Fig. 1

A semi-fragile watermark, which generated by the provider with equal tag to indicate the identity of website, was embedded into webpage. When a suspicious webpage came, the provider compared the generated and embedded watermark. If the inconsistence with the information was raised, the spoof webpage could be considered into a phishing page. The defeat phishing attack work done by the provider of website was called an active anti-phishing solution. The solution did not need end-users' confirmation and the detection criterion was done by the online sever, which was more accuracy than the heuristics-based methods. In the following, we shown the detail of active anti-phishing solution based on semi-fragile watermark.

Paypal website source code: <form method="post" name="login_form"action="https://www.paypal.com/c2/cgi-bin/webscr?cmd=_login-submit&dispatch=5885d80a13c0db1f8e263663d3faee8d5863a909c4bb5aeebb52c6e1151bdaa9">
Phishing site 1: <form method="post" name="login_form" action="webscr?cmd">
Phishing site 2: <form method="post" name="login_form" action="http://hackerdakhla.b4fh.com/scama/paypal/en/webscr?cmd">
Phishing site 3: <form method="post" id="login_form" action="post.php">

Fig. 1: Phishing activity in reality

ACTIVE ANTI-PHISHING SOLUTION

Solution hypothesis: Phisher lures end user to visit phishing site, the site also satisfy the following hypothesizes by our deep observation:

- **Hypothesis 1:** Phishing site impersonates well-known website by duplicating the whole or part of the target sites in order to show high visual similarity with its targets
- **Hypothesis 2:** The phishing site identity is inconsistence with the imitated website
- **Hypothesis 3:** In order to achieve user's information, phishing site always has a login form

Active anti-phishing solution exploits these hypotheses to defeat phishing attack. In this study, semi-fragile watermark embody these hypotheses. We show how the semi-fragile watermark generated method to embody these hypotheses lately.

Semi-fragile watermark generated method: The semi-fragile watermark is generated with formula 1.

$$W = h(cr||t||(t_1, t_2, t_3, t_4, t_5)||dn||url||sfh \quad (1)$$

where, h is a hash function such as MD5 or SHA-1; the symbol || is a concatenation symbol; symbol cr is the abbreviation of copy right; a flag t denotes the content of title tag; the tuple (t_1, t_2, t_3, t_4, t_5) contains five terms order by TF-IDF value in descent; symbol dn is the abbreviation of domain name; symbol url is an abbreviation of uniform resource locator appear in address bar; symbol sfh is an abbreviation of server form hander, its value is the content in server form hander.

Symbol cr and t and the tuple (t_1, t_2, t_3, t_4, t_5) embody to hypothesis 1; the symbol dn and url used in formula 1 embody in the hypothesis 2; sfh used to indicate the hypothesis 3.

Active anti-phishing solution architecture: According to hypothesis 1, phishing site always replicate whole or part of target's site source code to achieve visual similarity. So we can use active anti-phishing solution based on semi-fragile watermark to thwart the phishing attack by downloading the tactic's webpage and modifying a little to lure the victims.

The active anti-phishing solution departs into two parts: embedded part and detection part. In embedded part, a website service provider firstly generates semi-fragile watermark and embedded into webpage tag with equal tag idea to express the identity of website. The flowing chat of expressing the website identity is shown in Fig. 2.

The steps of this flow chat are given as follows:

Step 1: Generating semi-fragile watermark W with formula 1 of the protected webpage

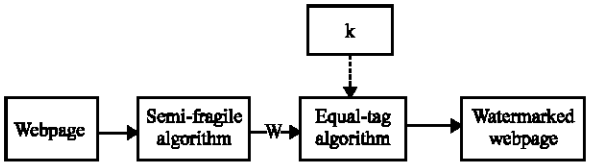

Fig. 2: The flowing of expressing the website identity

Step 2: Using ET embedding algorithm to embed the generated semi-fragile watermark with secret key k

Step 3: After the embedding step is done, the stego-webpage is output and deployed in the host of website

In the detection part, when a suspicious webpage came, the provider compares the generated and embedded watermark, if the inconsistence with the information is raised, the spoof webpage can be considered into a phishing page. The detection chat flowing is shown in Fig. 3.

The steps of this flow chat are shown in the following:

Step 1: Using TF-IDF algorithm to filter the unrelated suspicious webpage, only if the TF-IDF value is similarity to the protected website to sent to the step 2 and the others is output legal

Step 2: Using the formula 1 to generate semi-fragile watermark W'

Step 3: Using ET detection algorithm to extract the embedded semi-fragile watermark W''

Step 4: Compare semi-fragile watermark W' and W'', if they are consistence, then the flag phishing is output, else the flag legal is output

EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

Experimental results: Here, a semi-fragile watermark generated experiment was shown. Firstly, the homepage of PayPal and eBay was downloaded and the generated semi-fragile watermarks were list in Table 1 and 2. This information could be used to embed into the homepage with ET algorithm and could be represented the website's identity. If phisher downloaded the watermarked webpage and changed some place of the source code, the activity would be detected with active anti-phishing solutions.

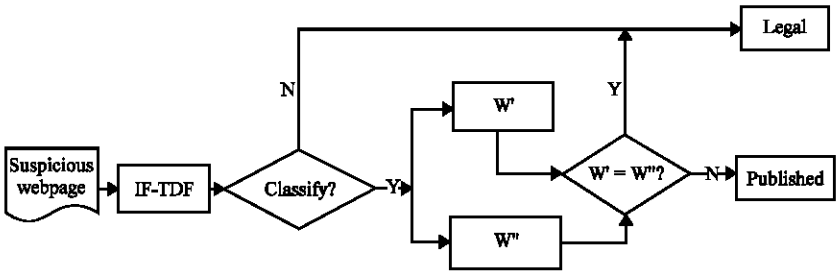

Fig. 3: The flowing of detection of phishing site

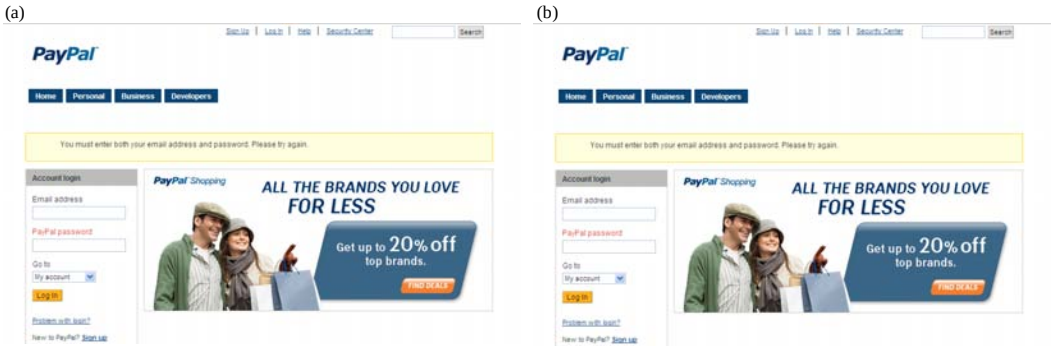

Fig. 4(a-b): The appearance of PayPal, (a) Without semi-fragile watermark and (b) embedding semi-fragile watermark

(a)

```
PayPal</LEGEND><LABEL for=3DsearchBox>Search </LABEL><INPUT =
id=3DsearchBox type=3Dtext=20
name=3DqueryString> <INPUT id=3DsayTminLength value=3D3 =
type=3Dhidden><INPUT id=3DcoDomain=20
value=3DUS type=3Dhidden><INPUT id=3Dsearch.x class=3Dbutton =
value=3DSearch type=3Dsubmit name=3Dsearch.x autocomplete=3D"off">=20
</FIELDSET> <INPUT value=3DUTF-8 type=3Dhidden name=3Dform_charset> =
</FORM>
```

(b)

```
PayPal</LEGEND><LABEL for=3DsearchBox>Search </LABEL><INPUT =
id=3DsearchBox type=3Dtext=20
name=3DqueryString> <INPUT value=3D3 id=3DsayTminLength =
type=3Dhidden><INPUT type=3Dhidden id=3DcoDomain=20
value=3DUS ><INPUT id=3Dsearch.x type=3Dsubmit class=3Dbutton =
autocomplete=3D"off" value=3DSearch name=3Dsearch.x >=20
</FIELDSET> <INPUT value=3DUTF-8 name=3Dform_charset type=3Dhidden> =
</FORM>
```

Fig. 5(a-b): The source code of PayPal, (a) Source code without embedding semi-fragile watermark and (b) Source code with embedding semi-fragile watermark

Using ET algorithm embedded the generated semi-fragile watermark into the protected website. Figure 4 was a snapshot of the PayPal homepage that imitate to protect without embedding semi-fragile watermark and embedding semi-fragile. Figure 5 was a part of the source code snapshot of Fig. 4. From the Fig. 4, it could find that the two homepages were similarity in appearance. So this solution more secret to the visible image watermark, because the phisher could not discover there had another protected way. The code underlined in Fig. 5 shown the difference between the two homepage. Though the source code was difference, the appearance was same in browser.

In order to verify the algorithm effectiveness, a phisher activity was imitated. By observation the phisher activity, the phisher only changed small place in order to preserve the same appearance. The place, such as server form handler or title's content, was changed. With this observation, two imitated phishing attack activities were done as follows:

Table 1: Semi-fragile watermark of PayPal

Parameters	Value
dn	PayPal
cr	1999-2011 PayPal. All rights reserved
t	Welcome-PayPal
url	https://www.paypal.com/am/cgi-bin/webscr?cmd=_home &locale.x=en_US
sfn	https://www.paypal.com/am/cgi-bin/webscr?cmd=_login-submit&dispatch=5885d80a13c0db1f8e263663d 3faee8db2b24f7b84f 1819390b7e2d9283d70f1
(t_1, t_2, t_3, t_4, t_5)	PayPal, shop, online, sign, pay
W	30-A2-52-E9-46-5A-67-3F-8B-9E-84-2B-54-33-02-DB

Table 2: Semi-fragile watermark of eBay

Parameters	Value
dn	eBay
cr	1995-2011 eBay Inc
t	eBay | Electronics, Cars, Clothing, Collectibles and More Online Shopping
url	http://www.ebay.com/
sfn	https://scgi.ebay. com/ws/eBayISAPI.dll? RegisterEnterInfo &siteid=0&UsingSSL=1&co_partnerId=2
(t_1, t_2, t_3, t_4, t_5)	ebay, video, new, center, cards
W	B6-64-19-A2-BF-9D-D1-EF-DF-51-0C-CC-75-ED-BC-C6

- Phishing attack #1 changed the source code content of action in form. For example, the code https://scgi.ebay.com/ws/eBayISAPI.dll?RegisterEnterInfo&siteid=0&UsingSSL=1&co_partnerId=2" was changed to "http://hackerdakhla.b4fh.com/scama/paypal/en/webscr?cmd"
- Phishing attack #2, not only changed the source code content of action in form as above but also changed the title content to "welcome PayPal"

After the two imitating phishing attack were done. The active phishing verified the phishing activity and listed the answer in Table 3. From the table, it could find that the semi-fragile watermark could be detect the phishing activity. So the active anti-phishing solution could be used to protect the owner of website.

Table 3: Phishing attack to PayPal

Identity	Phishing attack #1	Phishing attack #2
W'	5B-34-DD-5C-5F-C7-71-B9-78-B2-22-85-B1-31-0E-DB	D8-91-A3-4C-6D-2F-9E-C3-07-3D-E6-CA-A6-35-51-1C
W''	30-A2-52-E9-46-5A-67-3F-8B-9E-84-2B-54-33-02-DB	30-A2-52-E9-46-5A-67-3F-8B-9E-84-2B-54-33-02-DB
Result	Phished	Phished

Performance analysis: Firstly, the performance of the active anti-phishing solution analyze in usability, imperceptibility and security.

Usability: There have some anti-phishing approaches published in literatures with visible image watermark (Topkara *et al*., 2005; Huang *et al*., 2010; Singh *et al*., 2011). As they describe, a unique watermark to each end user embedded in image to show the website identity. So the end users just remember this unique image watermark and distinguish legal website or illegal website with that. Though those approaches provide a method to end user to verify website's identity with unique image watermark, end user always ignore this and then it make those solutions ineffective.

Our anti-phishing solution is developed to assist the owner of website to automatically distinguish phishing site but not manually in previous. The heuristic to verify phishing activity is the website provider actively embedded into the website source code. So the false negative of phishing detection is very small. Another advantage is that it is not dependent on the end user to distinguish phishing or not, which will avoid ignoring the warning flag to leak out personal information.

Imperceptibility: The active solution using equal tag method to embed semi-fragile watermark into webpage. Reference (Sun *et al*., 2007) has shown that this method wills imperceptibility to human. So the phisher would not find the downloaded webpage with identity information.

Security: As described above, the phisher will not to find the embedded information. When the phisher download the tactic site's source code, they only change small source code to cheat end user but not to destroy the embedded watermark. It will help the owner of website to confirm the phishing activity. So our approach is more security than the visible image watermark approaches, because of ours' will not incur the phisher suspicious.

CONCLUSION

Phishing was an important problem that results in identity theft. Although simple, phishing attacks were highly effective and have caused billions of dollars of damage in the last couple of years. In many cases, the phisher did not directly cause the economic damage but resell the illicitly obtained information on a secondary market. Hence, phishing attacks were still and important problem and solutions were required.

Phishers used the downloaded webpage from the real Web site to make the phishing webpage appears exactly the same as the real one did. An active anti-phishing solution was done by online service provider to protect end-users from making mistakes. The solution can effectively thwart the phishing attack by downloading the tactic's webpage and modifying a little to lure the victims.

ACKNOWLEDGMENT

This study is supported by National Natural Science Foundation of China (No. 61202496), Hunan Provincial Natural Science Foundation of China (No.10JJ4043, 10JJ5062), Hunan Province Planned Science and Technology Key Project (No. 2010NK2003), Hunan Province Planned Science and Technology Project (No. 2010TZ4012).

REFERENCES

APAC, 2011. Fishing site processing briefing. Anti-Phishing Alliance of China. http://www.apac.org.cn/gzdt/201112/P020111220573233390983.pdf

APWG, 2007. Phishing activity trends: Report for the month of November, 2007. Anti-Phishing Working Group. http://www.antiphishing.org/reports/apwg_report_nov_2007.pdf

Abbasi, A., Z. Zhang, D. Zimbra, H. Chen and J.F. Nunamaker, Jr., 2010. Detecting fake websites: The contribution of statisitical learning theory. MIS Quarterly, 34: 435-461.

CNERT/CC, 2010. 2009 Internet users in China network information security survey report. http://www.cert.org.cn/UserFiles/File/1.doc

Chen, T.C., S. Dick and J. Miller, 2010. Detecting visually similar web pages: Application to phishing detection. ACM Trans. Internet Technol., 10: 1-38.

He, M., S.J. Horng, P. Fan, M.K. Khan and R.S. Run *et al*., 2011. An efficient phishing webpage detector. Exp. Syst. Appli., 38: 12018-12027.

Hong, J., 2012. The state of phishing attacks. Commun. ACM, 55: 74-81.

Huang, C.Y., S.P. Ma, W.L. Yeh, C.Y. Lin and C.T. Liu, 2010. Mitigate web phishing using site signatures. Proceedings of the IEEE Region 10 Conference on TENCON, November 21-24, 2010, Fukuoka, Japan, pp: 803-808.

Huang, H.J., L. Qian and Y.J. Wang, 2012. A SVM-based technique to detect phishing URLs. Inform. Technol. J., 11: 921-925.

Khatibi, A., A. Haque and K. Karim, 2006. E-commerce: A study on internet shopping in Malaysia J. Applied Sci., 6: 696-705.

Singh, A.P., V. Kumar, S.S. Sengar and M. Wairiya, 2011. Detection and prevention of phishing attack using dynamic watermarking. Inf. Tech. Mobile Communi., 147: 132-137.

Steel, C.M.S. and C.T. Lu, 2008. Impersonator identification through dynamic fingerprinting. Digital Invest., 5: 60-70.

Sudha, R., A.S. Thiagarajan and A. Seetharaman, 2007. The security concern on internet banking adoption among Malaysian banking customers. Pak. J. Biol. Sci., 10: 102-106.

Sun, X.M., H.J. Huang, B.W. Wang, G. Sun and J. Huang, 2007. An algorithm of webpage information hiding based on equal tag. J. Comput. Res. Dev., 44: 756-760.

Topkara, M., A. Kamra, M.J. Atallah and C. Nita-Rotaru, 2005. ViWiD: Visible watermarking based defense against phishing. Proceedings of the 4th International Workshop on Digital Watermarking, September 15-17, 2005, Siena, Italy, pp: 470-483.

Xiang, G., J. Hong, C.P. Rose and L. Cranor, 2011. CANTINA+: Feature-rich machine learning framework for detecting phishing web sites. ACM Trans. Inf. Syst. Secur., 14: 21-48.

Zhang, H., G. Liu, T.W.S. Chow and W. Liu, 2011. Textual and visual content-based anti-phishing: A Bayesian approach. IEEE Trans. Neural Networks, 22: 1532-1546.