Poster: Anti-Phishing system using footprint-sharing web site

Eri Otsuka
Kanagawa Institute of Technology
Shimo-ogino 1030 Atsugi-shi
Kanagawa, Japan

Ayaka Miyazawa
Kanagawa Institute of Technology
Shimo-ogino 1030 Atsugi-shi
Kanagawa, Japan

Manabu Okamoto
Kanagawa Institute of Technology
Shimo-ogino 1030 Atsugi-shi
Kanagawa, Japan
manabu@nw.kanagawa-it.ac.jp

1. INTRODUCTION

Phishing becomes a serious threat [1]. Especially it is a menace for low-literacy users like a child and an old person.

Phishing is a criminal mechanism to steal consumers' identity data like name or address or age or id/password or financial account credentials. Phishing site sends spoofed e-mails which pretend to be from legitimate web site and lead users to come to web sites. Deceived recipient clicks the link on e-mail and visit the site which is designed as same as right site. Fake site tricks visitors into inputting personal data such as usernames and passwords. So these personal data is stolen. There are thousands of fake phishing websites established online every day, luring any number of consumers to trouble and loss.

Phishing attacks remain at high levels, with some 20,000 to more than 25,000 unique phishing campaigns recorded each month though the half [1]. SSL or security software are used to prevent phishing. It is effective for high-literacy users, but for low-literacy users these techniques are difficult to manage.

In this paper we propose new anti-phishing method which is simple and easy to manage for low-literacy users.

2. RELATED WORK

We can use Black list or White list to confirm whether that site is Phishing site. But Black/White list method has some issues.

To use White list we have to update the list quickly when new site open. Similarly to use Black list we have to update the list quickly when new Phishing site is found. But life time of Phishing site is short ,so when we add the site to list, the site may be disappeared and the list may be ineffective.

And it is also difficult to distribute these lists. We need also security software [2][3] to use Black/White list. These softwares show us suspicious sites on the browser or alert pop-up. We need to update the list frequently to use the latest list on these security softwares. On-line PC is easy but off-line PC is difficult. The biggest problem is that we have to install these softwarse. It is difficult for a child and an old person.

Yahoo! Japan's Login-seal [4] is pretty good idea. Users can set a personal seal which consists of character string and an image the user selects. This seal is displayed on login form. Before inputting ID and password, users can check whether that seal is same as my seal. Phishing sites do not know what seal the use had and so they cannot display right seal there. But this seal is stored in browser cookie. So if you delete the cookie or you use another PC, you cannot use Login-seal. And that seal is personal, so you cannot use this seal on sharing PC. And configuration for setting seal is difficult for a child and old person. Figure 1 shows Login-seal.

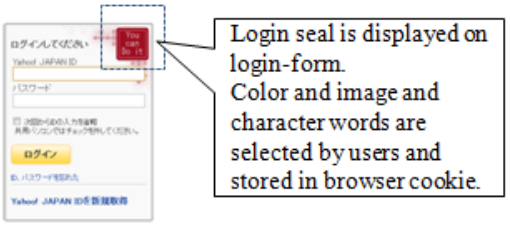

Figure 1. Login seal of Yahoo!Japan.

3. PROPOSED METHOD

In this section we propose anti-phishing system that uses footprint-sharing web site. In this method we need no install and no distribution of Black/White list and no cookie and no configuration. It is easy for all users including a child and an old person.

What is footprint? We call personal access log 'footprint'. For example when Alice push the link 'go to site B' and visit the site B, then 'Alice leave footprint on site B'.

In this method 'footprint button' is displayed in the login form and in order to check whether this site is phishing site, users push the button. This button is simple link to the footprint-sharing web site.

We think that users will not have trouble to push the button because it is likely the Like button in facebook [5] (Figure 2).

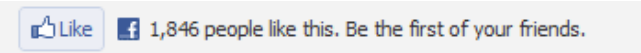

Figure 2. Like Button

Here, we describe the steps in our proposed scheme.

1) Alice visits the Service Provider. She wants to login and use the site service. And she wants to check whether this site is not fake.

2) Before Alice input ID/Password into the login form, she pushes the footprint button. Figure 3 shows the example.

3) The footprint button is link to the footprint-sharing site and the browser moves to that site. Maybe new window is opened and that site is displayed in the new window.

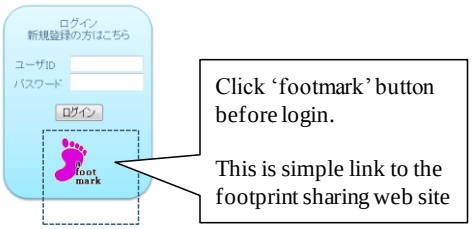

Figure 3. Footmark button.

4) The footprint-sharing site gets the http-Referrer URL and check the URL. Maybe the footprint-sharing site uses Black list or White List. But in this paper we do not refer to how to check the URL. We can use any methods to check the URL freely. Black/White list is stored only in the footprint-sharing site and users need not to have them on their PC.

5) The footprint-sharing site shows the result for Alice. It is OK or Suspicious ,and so Alice can check easily.

6) If it is OK, Alice goes back to the Service Provider and input ID/Password in the form.

Figure 4 shows the sequence of this scheme.

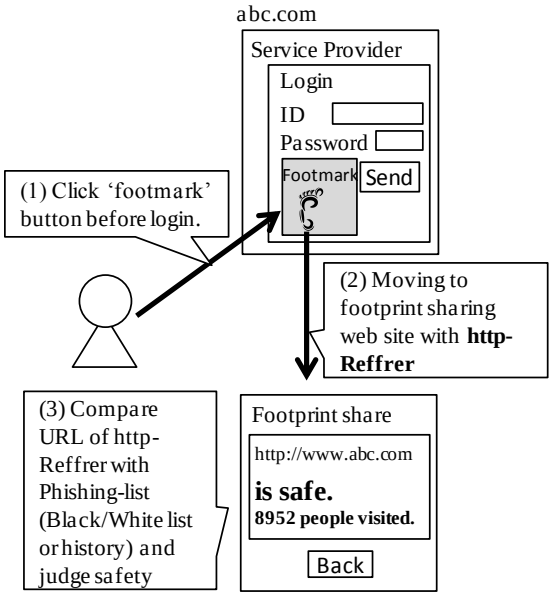

Figure 4. Sequence of proposed method.

In step 4 we can use the history of visiting the site to check whether the site is phishing site. When all users share the history, Alice can confirm whether she visited the site is same as the site that other majority of people visited. When Alice uses her personal history, Alice needs to login the footprint sharing site. Then she can confirm whether she visited the site same as the site that she ever visited once. For example Alice usually uses the sites and leaves many footprints at home and one day Alice goes out for business and uses hotel sharing PC. She can confirm the footprint which she leaves now at hotel is same as ones which she had left at home.

When we use history to confirm Phishing sites, we need no Black/White lists. And history list is made automatically, so we need not to update lists.

4. SECURITY ANALYSIS

In this section, we describe good points of our method.

Usability: In this scheme, we need no install no configuration, no cookies. It is very simple and easy also for a child and old person. And we can use this scheme in sharing PCs. We need to push the 'footmark button' and so the click number of times increases, but it is not surely a great problem as same clicking 'Like it' button.

Efficiency: We need not to distribute Black/White lists for clients. If we use history of footmarks, we need not to update lists. For service provider using this method, they do only add the link of footprint-sharing web site at their HTML. It is very easy and need no money.

Security: If the footprint sharing web site is also Phishing site, do we deceive? When the footprint sharing web site is fake, they can display 'this site is OK" on the fake site. We think that the footprint sharing web site needs any other strong anti-Phishing technique like EV-SSL. EV-SSL is strong but so expensive for poor web site. But by using our scheme, poor web site can rely on footprint-sharing web site which is strong for Phishing.

5. CONCLUSION

In this paper, we proposed an anti-Phishing system using footprint-sharing web site. Users only need to push the footprint button which is link to footprint-sharing web site. The footprint-sharing web site checks the http-Referrer header and show whether that URL is OK or Phishing site. In this method users need not any install and any configurations. And users can use this system on sharing PCs.

6. REFERENCES

[1] Anti-Phishing Working Group (APWG), http://www.antiphishing.org/.

[2] Browser Defender, http://www.browserdefender.com/.

[3] McAfee SiteAdvisor , http://www.siteadvisor.com/.

[4] Yahoo! Japan, https://www.yahoo.co.jp/.

[5] facebook, https://www.facebook.com/.

[6] Downs, J., M. Holbrook and L. Cranor, "Decision strategies and susceptibility to phishing," In Proceedings of the Second Symposium on Usable Privacy and Security (SOPUS'06 Pittsburgh, Pennsylvania, July 12 - 14, 2006), vol. 149, pp.79-90, ACM Press, New York.

[7] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru,Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, Elizabeth Nunge, "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish," In Proceedings of the Second Symposium on Usable Privacy and Security (SOPUS'11 Pittsburgh, Pennsylvania, July 20 - 22, 2011), ACM Press, New York.