# Poster: Anti-phishing System
# Link-back to Login Page from Footprint

Saki Naguchi
Kanagawa Institute of Technology
Shimo-ogino 1030 Atsugi-shi
Kanagawa, Japan

Nami Hidaka
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 is a criminal mechanism to steal consumers' identity data such as an id/password or financial account credentials. Spoofed e-mails lead users to fake web sites designed to look the same as the real site. The fake site tricks visitors into inputting their ID/password and the input data are stolen.

We proposed a new anti-phishing method at SOUPS'12 [1]. In this method, before inputting an ID/password, a user clicks the "foot-print" button that is a link to the "footprint-sharing web site". The footprint share web site checks the URL of http referrer by comparing it with a black/white list or history.

But this method encounters a problem when the footprint-sharing web site is also a fake site. So, we improved our method and by using a smartphone and link back to the login page we can login to the correct site more safely.

## 2. RELATED WORK

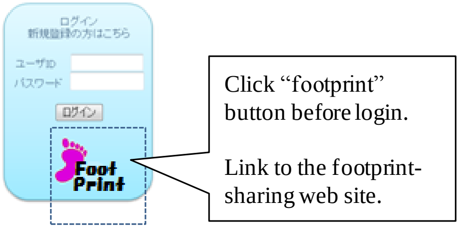
We can use a black list or a white list to confirm whether a site is a phishing site. But, we always have to update the black/white list. The black list lifetime of a phishing site is especially short, so by the time we add the site to the list, the site has disappeared and the list is ineffective. It is also difficult to distribute these lists and we need to install security software, which shows us suspicious sites on the browser or an alert pop-up. We need to continue using the same PC installed with this software and the latest black/white list. When we use another PC, for example, the business center in a hotel, we cannot use these methods.

In [1] we proposed an anti-phishing system that uses a footprint-sharing web site. In this method, we need no installation software, no distribution of a black/white list, and no configuration. We call the personal access log a "footprint". For example, when Alice pushes the link "go to site B" and visits site B, Alice then leaves a footprint on site B.

The footprint button is displayed in the login form, as shown in Figure 1, and to check whether this site is a phishing site, users push the button. This button is a simple link to the footprint-sharing web site.

The browser goes to the footprint-sharing site, gets the http referrer URL, and checks the URL by comparing it with the black list or white List, or the history of all users. The black/white list is stored only in the footprint-sharing site and users do not need to have these lists on their PC. The footprint-sharing site shows the result.

But a problem occurs in one situation. A fake site shows a fake footprint button and leads users to the fake footprint-sharing site. It incorrectly displays to users "This is a safe site." We can avoid this attack by an EV-SSL of the footprint-sharing site, but it is not effective.



Click "footprint" button before login.

Link to the footprint-sharing web site.

**Figure 1. Footprint.**

## 3. PROPOSED METHOD

In this section we propose a new anti-phishing system that uses a footprint-sharing web site. We improve our method by using a smartphone and link back to the login page, where we can safely check whether it is the correct site.

Here, we describe the new steps in our proposed scheme. A figure 2 shows the sequence of this scheme.

1) Alice visits the service provider (SP). She wants to login and use the site service. In addition, she wants to check that this site is not fake.

2) Before Alice inputs her ID/Password into the login form, she pushes the footprint button.

3) The footprint button is a link to the footprint-sharing site and the browser goes to that site. A new window may be opened and that site is displayed in the new window.

4) The footprint-sharing site gets the http referrer URL and checks the URL. The footprint-sharing site uses the black list, white list, or history list of all users. In this paper, we do not discuss how to check the URL. We can use any method to check the URL. The black/white list is stored only in the footprint-sharing site and users do not need to have them on their PC.

5) The footprint-sharing site shows the event that a user visited it from the SP. Alice has connected to the footprint-sharing site with a smartphone or tablet PC before step 1 and keeps updating the event automatically by browser add-on software. On the smartphone or tablet PC, Alice can connect to the correct footprint-sharing site because she can connect by a bookmark that was confirmed in the past. All events are showed on the site. But the event in which Alice visited the SP may be buried in many other events. At that time we can filter it by a hash-

tag, such as #john123, which Alice inputs when she connects to and leaves the footprint at the footprint-sharing site, as shown in Figure 3. Of course, the hash tag may be the same one used by others coincidentally. But, we use it only for filtering and so we can pick the target event easily.

6) The footprint-sharing site makes a link back to the login page of the SP. This is just a link to the login page of the SP and it is made by using safe information that the footprint-sharing site has in its database. The footprint-sharing site gets http refferer and picks the link back to the URL from the database comparing the URL of http refferer.

7) Alice clicks "Link back to login page of SP".

8) The browser moves back to the login page of the SP. This is a safe URL.

A Figures 4 also show the sequence of this scheme.

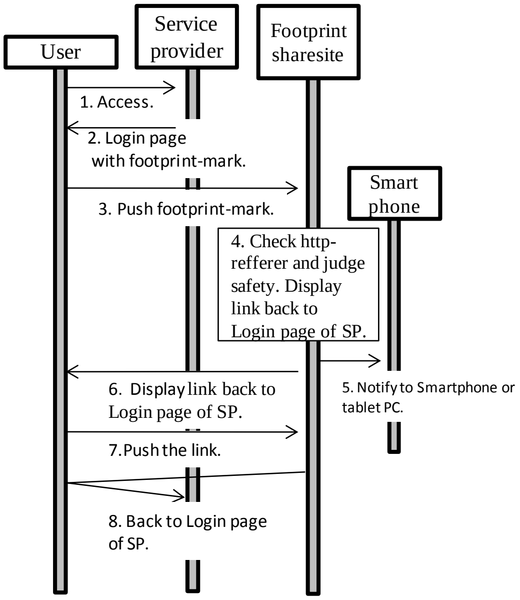
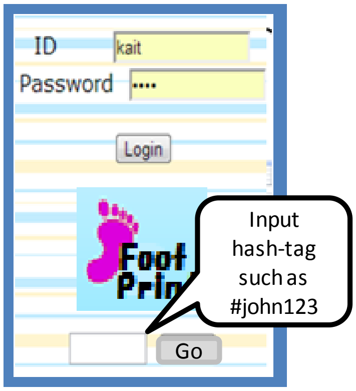

User
Service provider
Footprint sharesite
Smart phone
1. Access.
2. Login page with footprint-mark.
3. Push footprint-mark.
4. Check http-refferer and judge safety. Display link back to Login page of SP.
5. Notify to Smartphone or tablet PC.
6. Display link back to Login page of SP.
7.Push the link.
8. Back to Login page of SP.

**Figure 2. Flow of proposed method.**


ID kait

Password ••••

**Figure 3. Illustration of proposed method.**

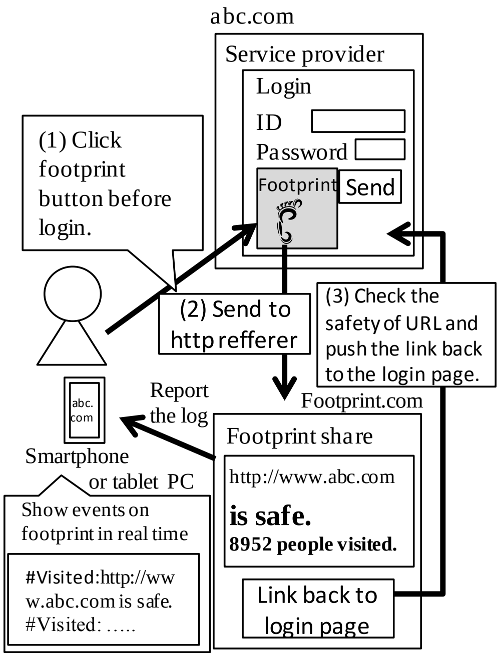


**Figure 4. Detail of proposed method.**

## 4. ADVANTAGES

In this scheme, clients need no install, no configuration, no cookies, and no distributing of black/white lists. The service provider only needs to add the link of the footprint-sharing web site in its HTML. Users connect to the footprint-sharing web site in parallel from a safe bookmark and keep updating the event on that site. When a PC connects to a fake SP and is lead to the fake footprint-sharing web site, no event occurs on the smartphone or tablet PC, and so the user notices it.

## 5. CONCLUSION

In this paper, we proposed an improved anti-phishing system using a footprint-sharing web site. Users need only to push the footprint button, which is a link to the footprint-sharing web site that checks the http referrer header. By checking the event on the footprint-sharing web site with a smartphone or tablet PC in real time, we can trust the footprint-sharing web site.

## 6. REFERENCES

[1] Otsuka, E., Miyazawa, A., and Okamoto, M. 2012. Anti-phishing system using footprint-sharing web site. Poster. Symposium On Usable Privacy and Security (SOUPS2013).

[2] Downs, J., Holbrook, M., and Cranor, L.. 2006. Decision strategies and susceptibility to phishing. In Proceedings of Symposium On Usable Privacy and Security(SOUPS2006).

[3] Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.C., Hong, H., and Nunge, E. 2011. Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In Proceedings of Symposium On Usable Privacy and Security (SOUPS2006).