Hierarchy OpenID

DONGHWI SHIN, INKYUN JEON, HYUNCHEOL JEONG
Security Technology Team
Korea Internet and Security Agency
IT Venture Tower, Jungdaero 135, Songpa, Seoul
Korea
shindh@kisa.or.kr, ikjeun@kisa.or.kr, hcjung@kisa.or.kr

Abstract: - The explosive developments of web services provide convenience of anytime, anywhere the service for users. However, the evolution of web service to its users provides the burden of a number of identity and password pair management. To solve such a problem that emerged was openid. The key concept of openid is to manage only one ID for user convenience. Therefore, openid user manages only one identity when the user requests service from the service provider, that supports openid. However, due to openid concept with openid protocol, some security issue is appeared. In this paper, we propose the Hierarchy OpenID concept as a solution to the openid security issue.

Key-Words: - Openid, Security, Phishing, Linkability, Traceability, Authentication

1 Introduction

With web development, many services have moved to web. Accordingly, users are using a variety of services on the web. However, in order to receive services from the service provider(SP) users authenticate from SP. The commonly used method for authenticating is the ID/Password method. However, with the increase in SP, the user needs to manage the increased number of ID for authentication. Therefore, this causes inconvenience of the number of user identity and password pair management. The openid is appeared to alleviate the inconvenience. The openid main concept is to minimize the number of Identity.(By default, user manages only one openid in openid service.) While providing the convenience of an identity management for users, openid provider and SP, supports openid, has also increased. According to the web 2.0 paradigm, the user's movement affects SP. Major portal site started to support openid. And currently Google, Yahoo, Microsoft has issued both openid.

However, some security issues are caused by reduction of the number of identity that user manages. Because of openid protocol emergence, some security issues are appeared too. In this paper, we present solutions for openid security issues, which are the openid provider phishing, identity linkability and traceability problem. Also, we present our scheme to resolve the current openid anonymous service problem.

The remainder of this paper is structured as follows. Section 2 describes openid service, openid security issue. Section 3 proposes our hierarchy openid scheme. Finally, conclusions are drawn in section 4.

2 The present state of OpenID

2.1 openid Service

In the introduction, we mentioned that the openid main concept is to minimize a number of identities the user manages. The openid chooses a URL to uniquely identify a web user. This means that the user was aware of the resources. Also, this means the end users involved in the authentication mechanism.

The components for openid service are user, service provider(SP), and openid provider(OP). (However, the existing service provider performed both the role of SP and the role of OP.) And all authentication information is passed through the user. The following is openid protocol.

□ Send user openid to SP or OP domain, which the user issued from.
The some OP provides the anonymous openid for the above linkability and traceability issue. Thus, by using the anonymous openid it is hard to get the user information using openid linkability and traceability property. However, the anonymous openid generated by OP is changed to the random string form, the user can not remember, for the linkability and traceability issue solution. In addition to some anonymous openid is not true anonymous openid. Because the anonymous openid does not be changed, though the anonymous is the complicated string. In addition, the user can not choose the level of anonymous because the OP provides the anonymous property of an anonymous openid.

3 Hierarchy OpenID

In this paper, we propose hierarchy openid to resolve openid security issue mentioned earlier in Section 2. The main concept of the hierarchy is the classification of the user's openid. This section mentions the concept of hierarchy openid and issues for applying the hierarchy openid in terms of the user, SP, OP on the openid authentication mechanism. Finally, this section describes how to resolve the openid security issue through the hierarchy openid scheme.

3.1.1 Hierarchy OpenID Scheme

The hierarchy openid provides the user with two types openid.

① Parent OpenID(1st ID or Closed ID)
② Child OpenID(2nd ID or Opened ID)

The parent ID(1st ID) is the id that is used to sign up for OP at first time. This parent ID is not a public openid as ID for the management of the user child openid(2nd ID). The 2nd ID is a public openid as ID to get service from the SP on the authentication mechanism. The 2nd ID is dependent on the 1st ID that has unique properties on OP. And the 2nd ID among the ID belongs to the 1st ID must be unique. Though the opened or closed properties of the 1st ID or 2nd ID can be changed by the user, but is not
recommended. (When the opened or closed properties are changed, the authentication mechanism is described in the next section.) The reason is that the property of each ID has to do with openid security issue. Basic hierarchy openid scheme is as follows.

1. User joins in OP. OP issue the parent openid(1st ID)
2. User logs in with 1st ID
3. User sets the child openid(2nd ID)
4. User requires a service from SP and enters OP domain to SP opened login form.
5. SP redirects users to OP
6. User enters 1st ID and password to OP
7. User selects 2nd ID, is used to log in SP

Second, the 1st ID method is used when the user tries to log in the SP with 1st ID for the service from SP.

1. SP redirects user to OP with 1st ID
2. Select ID type(1st ID or 2nd ID. In this step, ID type is 1st ID)
3. Enter user password at OP authentication web page
4. OP shows 2nd ID list. Users selects 2nd ID that is used to log in SP

However, the scenario will change slightly when the user is using the domain name method. In case of the 1st ID method, the user enters 1st ID to SP. But in domain name method the user enter the 1st ID to OP because the user redirect to the OP without input the 1st ID. After the 1st ID is entered on the domain name method, and then the next process is the same as the 1st ID method. However, the 1st ID method is not recommended. The reason, that the 1st ID method does not recommend, is that the 1st ID property is changed to "Opened" for 1st ID method. This comes into collision with objective that aims to resolve the linkability and traceability issue by setting 1st ID property to "Closed".

3rd, 2nd ID method is the case of that user input the 2nd ID to log in the SP in the service requests from SP.

1. SP redirects user to OP with 2nd ID
2. Select ID type(1st ID or 2nd ID. In this step, ID type is 2nd ID)
3. Enter the 1st ID and password

When considering convenience and reality, what does not enter the 2nd ID will be effective. Because the 2nd ID in addition to other 2nd ID may already have been submitted to the SP and you don’t remember it, if the user has visited in SP. With 2nd ID list of URL, the SP manages, because OP shows the list the URL. no matter what the 2nd ID input of the user. We recommend what does not input the 2nd ID.

The 2nd ID method has also the other issue. The 2nd ID that the user owns is only a unique in the 1st ID area, but the 2nd ID is not unique in the entire ID space. The 2nd ID entered by the user may be one of the 1st ID using by the other user. (Because the basic properties of the 1st ID is closed and the property change is not recommended, the probability is extremely small. But the probability is not zero.) Therefore, OP is able to distinguish the ID(1st ID or 2nd ID) is entered by the user.
3.1.3 Hierarchy OpenID Information Table

Hierarchy OpenID provides a different ID type. Therefore the OP manages 1st ID user table and 2nd ID table for each user for the hierarchy OpenID service implementation.

First, the 1st ID table of the user is 1st ID management table and primary key of the table is the 1st ID. The elements of 1st ID table are as follows.

- 1st ID
- number of 2nd ID on 1st ID space
- Password
- …

<table>
<thead>
<tr>
<th>1st ID</th>
<th># of 2nd ID</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>3</td>
<td>Encrypted string</td>
</tr>
<tr>
<td>BBB</td>
<td>6</td>
<td>Encrypted string</td>
</tr>
<tr>
<td>CCC</td>
<td>4</td>
<td>Encrypted string</td>
</tr>
</tbody>
</table>

Fig5. 1st ID table

The number of 2nd ID element shows the number of 2nd ID included in the 1st ID. In addition, this element in the 2nd ID method will be used for verification. When modifying the hierarchy OpenID scheme, it will be available.

Second, the 2nd ID table is a table for 2nd ID, depend on a 1st ID, management and primary key of the table is the 2nd ID. The elements of 2nd ID table are as follows.

- 2nd ID
- Password on 2nd ID(Optional)
- Usage count on site
- Site list
- Usage count on 2nd ID
- 2nd ID property(Opened / Closed, Default : Opened)
- …

<table>
<thead>
<tr>
<th>2nd ID</th>
<th>Password on 2nd ID</th>
<th>Usage count on site</th>
<th>Site List</th>
<th>Usage count on 2nd ID</th>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Encrypted string</td>
<td></td>
<td><a href="http://www.a.com">www.a.com</a></td>
<td>4</td>
<td>Closed</td>
</tr>
<tr>
<td>BBB</td>
<td>Encrypted string</td>
<td></td>
<td><a href="http://www.b.com">www.b.com</a></td>
<td>3</td>
<td>Closed</td>
</tr>
<tr>
<td>CCC</td>
<td>Encrypted string</td>
<td></td>
<td><a href="http://www.c.com">www.c.com</a></td>
<td>1</td>
<td>Closed</td>
</tr>
</tbody>
</table>

Fig6. 2nd ID table

Finally, the 2nd ID property element represents an "Opened or Closed" property of the 2nd ID. The 2nd ID will expose to the outside world in default setting. (Default value : closed) The “Closed” property means that the user can not use this ID on the authentication method. This “Opened or Closed” property does not mean a public property. However, if the user does not want to the closed property, the user can change this property and can use the 2nd ID method (The 2nd ID method is not recommended.).

3.1.4 OpenID Security Solution by Hierarchy OpenID

In 2.2 openid security issue section, we describes the following three issues.

- Phishing
- Linkability and Traceability
- Anonymous OpenID

First, the phishing problem can be solved through a combination 1st ID with 2nd ID. By default, the 1st ID does not disclosed to outside. And the 2nd is disclosed to outside and depend on 1st ID. Assume that an attacker implement the phishing OP site. When domain name method and the 1st ID method is used to log in to the OP, if the user has the normal OP to the list will show the 2nd ID list. However, the phishing OP can not show a normal 2nd ID list because the phishing OP does not know the 2nd ID list of user. And then the user can recognize the OP site is not normal. When the user enter the 2nd ID for the 2nd ID method, the phishing OP can not distinguish ID.
type(1st ID or 2nd ID). Therefore, any authentication method can prevent phishing OP.

Secondly, the linkability and traceability issues can be resolved through the property of the 1st ID 2nd ID, too. Though 2nd ID is published on the outer, there is some users using the same ID that is equal to 2nd ID of the user. Thus, even if any attacker tracks a user based on the 2nd ID, the attacker can not check the user, is interested in tracking, out. As well as the trace with other information collected don’t consider. A user can change the 1st ID. By default, because the 1st ID do not disclose outside, anyone can not trace the user through the 1st ID. Therefore, the hierarchy openid does not have a linkability and traceability issue.

Finally, the hierarchy openid can solve anonymous openid problem easily. Now OP provide the user with the anonymous openid and make it difficult. (The difficult means that it is difficult to remember the anonymous.) And the anonymous openid does not have a real anonymous property. However, the hierarchy openid can provide the user with an anonymous property using the 2nd ID. Because the 2nd ID is dependent on the 1st ID and a user does not have the limitations of the 2nd ID space. Also, the usage information of the 2nd ID in the 2nd ID table can be found directly. Finally, the 2nd ID was used appropriately for the anonymous openid and the user can adjust the anonymous level by deleting the 2nd ID. Therefore, through the hierarchy openid anonymous openid issue also is able to resolve

4 Conclusion and Future Work
So far, with the hierarchy openid scheme we mentioned the resolution for some openid security issues with this scheme. Of course, there is some OP (security) policy issue is including the restriction of number of possible 2nd ID. In addition, this scheme needs to make up for other details of the service scenario. Also the information should be managed identity and the identity management facility will be on the side of the OP and the SP. But if recently the participation of web users and users as a single service object are considered, the hierarchy openid will be able to be safely and effectively self-management service.

References:
[3] OpenID Authentication 1.1,

http://openid.net/specs/openid-authentication-1_1.html, 2008