Trust Management for User-Centric Identity Management on the Internet

Daeseon Choi, Seung-Hun Jin and Hyunsoo Yoon

Abstract — In user-centric identity management, user select IDP. There is no relationship between the IDP and the relying web site. To evaluate the credential presented by a user and issued by the IDP, the relying web site has to decide to trust the issuer IDP. As the types of identity information provided by IDPs are various, it is very difficult for a TTP to gather and manage trust of all kinds of IDP. To solve this trust management problem, we propose reputation based trust management method. In our method, web sites that have experience of the IDP vote for the trust of the IDP. There is single TTP for aggregating the vote and transmitting the vote result to the relying web site. With this method, the relying web site can get the information for deciding trust of IDP that is unfamiliar to the web site.

Index Terms — Identity Management, User-Centric, Trust Management

I. INTRODUCTION

Identity management on the Internet is hot issue in today. Providing capability of management of distributed identity information over the Internet web site and making it convenient to register id and password and to memorize and use it in many web site are objectives of the Internet identity management.

To solve this problem, many approaches have been being tried last years. They are centralized approaches, federated approaches and user centric approaches. The representative centralized approach is Microsoft .Net passport[1]. In the passport solution, a centralized identity provider presents authentication assertion and attribute of users. This approach has problem of monopoly of service and integration of private identity information. Microsoft has dropped the .Net passport service recently. In federated approach, Internet web sites federate and share their users’ identity. Different identifiers of one user at different web sites are linked each other by user itself. After the identifiers are linked, authentication is able to be shared among the web sites by exchanging authentication assertion to provide the Single Sign On function.

User centric identity management approach is proposed to overcome the shortcomings of previous approaches and to make the adaptation range bigger. Figure 1 shows the basic concept of user centric identity management.

<table>
<thead>
<tr>
<th>IDP</th>
<th>credential</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td></td>
</tr>
<tr>
<td>Web Site</td>
<td></td>
</tr>
</tbody>
</table>

Figure 1. Overview of the user centric identity management

In user centric approach, a user selects an IDP that he wants without the restriction made by whether a web site that the user is visiting has federation relation with the IDP. The user takes some credential that contains some identity information such as personal profiles is being used to provide customized service and to keep up-to-date information. The representative federated approach is Liberty Alliance ID-FF and ID-WSF specifications[2][3]. With federated approach, user can use the identity management service on the boundary of federated web sites. A web site accepts only the assertion issued by an IDP or other web site that it has made federation. If the user has not register the IDP, the user can not use the identity service such as SSO on the web site, even thought he had registered in some other IDP. It is same situation of credit card. If a store accepts only one kind of credit card, consumer who has some credit cards other than that kind can not pay with credit card.

User centric identity management approach is proposed to overcome the shortcomings of previous approaches and to make the adaptation range bigger. Figure 1 shows the basic concept of user centric identity management.

<table>
<thead>
<tr>
<th>IDP</th>
<th>credential</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td></td>
</tr>
<tr>
<td>Web Site</td>
<td></td>
</tr>
</tbody>
</table>

Figure 1. Overview of the user centric identity management

In user centric approach, a user selects an IDP that he wants without the restriction made by whether a web site that the user is visiting has federation relation with the IDP. The user takes some credential that contains some identity information such as personal profiles is being used to provide customized service and to keep up-to-date information. The representative federated approach is Liberty Alliance ID-FF and ID-WSF specifications[2][3]. With federated approach, user can use the identity management service on the boundary of federated web sites. A web site accepts only the assertion issued by an IDP or other web site that it has made federation. If the user has not register the IDP, the user can not use the identity service such as SSO on the web site, even thought he had registered in some other IDP. It is same situation of credit card. If a store accepts only one kind of credit card, consumer who has some credit cards other than that kind can not pay with credit card.

By the way, a new problem occurs in the user centric approach. That is how a web site trust the information contained in the credential that the user submitted. It is problem of how to trust an IDP that issues the credential. In contrary to the federated approach, the web site doesn’t have...
any relation with the IDP. So the website doesn’t have any criteria for deciding whether it accepts the information contained in the credential or not, in other words, whether it trust the issuer of the credential or not. This is the main problem that this paper intends to present a method to solve.

The information contained in a credential is various. Authentication assertion for SSO is one of them. And many types of user attributes are others. Trust of the IDP can be various for the type of information that the IDP issued credential contains. There is the situation that an IDP can be trusted for authentication assertion but it can not be trusted for providing the user’s financial credibility. So the trust of an IDP has to be managed and evaluated for the each type of information that the IDP provides.

This paper suggests a method for solving this problem that is management of trust in the user centric identity management. This paper is organized as follows. Section represents previous work that is related with this problem. The reason of using the term “related” is that there is not any previous research that has tried to solve this problem exactly. In Section III, we proposes our approach to solve the problem. The architecture and manner of our method are presented. Finally, we conclude with outlook in Section V.

II. RELATED WORKS

A. Trust management in user-centric identity management approaches

The representative user-centric identity management is OpenID[4] and Microsoft Cardspace[5] currently. The trust management defined in this technology can not solve the proposed problem. In the OpenID, relying web site make secure association using Diffie-Hellman key agreement. This process doesn’t provide the trust of transmitted information. And it does not provide even entity authentication. It only provides the message integrity between IDP and relying web site. The Microsoft Cardspace uses public key certificate and SSL for authenticating between IDP and relying web site. It also does not guarantee the trustworthiness of the information provided by the IDP.

B. Trust evaluation based on the TTP

Other approach to evaluate trust between entities that have not any previous relationship is to depend on the information from a third party authority. In this approach, a authority makes and keep track of trustworthiness of all IDPs. The trust information of the authority is transmitted to the relying web site via one of three methods shown in the Figure 2.

Figure 2. Trust evaluation based on the TTP

III. PROPOSED METHOD

To provide trust evaluation of the IDPs in the environment of no previous trust relationship existing and IDP providing various types of information, we propose reputation based trust evaluation approach. In our method, the web sites that have used credential issued by an IDP provide the trust information to the relying web site that has never experience the IDP previously. Our method consists of the system architecture and operating procedure.

A. Architecture

Proposed method’s system architecture is shown in the figure 3. There are an aggregation TTP, some voting web sites and a relying web site.

- Aggregation TTP

It is some kind of voting management system. It aggregates votes from voting web site and calculates result of voting. When relying web site queries the trustworthiness of an IDP, it provides the calculated result. It has responsibility of keeping not distorted reputation from voting web sites. It means that the aggregation TTP has to prevent some malicious voters from distorting the result. But it has not to influence the trustworthiness of an IDP by itself.
Relying Web Site

The relying web site trusts the Aggregation TTP. When a credential is submitted by a user, it evaluates the trustworthiness of credential’s issuer by transmitting the Trust Query to the aggregation TTP. If the relying web site has enough experience of the IDP, it is not necessary to query. The query result is not decision of yes or no. The query result is a measure of trustworthiness. Decision of trust or not is made by the relying web site based on the measure from query result. Relying web site has some threshold for deciding trust. This threshold is various for the type of information and the usage of the information. On the case of validity of information in a credential is high, the threshold value is set as high also.

Voting Web Site

After processing a credential issued by an IDP, the relying web site has experience about the issuer. Based on this experience, the web site votes the trustworthiness of the IDP. The experience grows positively for each credential processing case. It assumes that the IDP’s activity is good. When the relying party finds out that the information from an IDP is wrong by a certain way, it dismisses its positive experience of the IDP and has the negative experience. It transmits its experience to the aggregation TTP.

Trust Query

There are trust query message and result message. The query message contains following items.
- IDP: identifier of the evaluated IDP
- Type: type of information contained in the credential issued by the IDP

The result message consists of following fields.
- Trust measure: aggregation result of votes
- Signature: signature of the aggregation TTP

B. Implementation

Figure 4 shows the software architecture of the system implementing the proposed method

Aggregation TTP
- Aggregation Module: collect and filter votes from web site
- Publishing Module: query process module

Web Site
- Voting Module: transmits vote to the aggregation TTP
- Credential Consuming Module: after consuming credential, experience is gathered
- Credential Evaluation Module: query to the aggregation TTP and evaluate IDP’s trust based on the query result
IV. CONCLUSION

In this paper, we proposed the reputation based trust evaluation method for relying web site in the user centric identity management environment. With our method, the relying web site can evaluate the unfamiliar IDP that the user selects based only the trust of the aggregation TTP. This method contributes to make the user centric identity management adaptation large.

The research about classification of types of identity information and method of preventing malicious conspiracy of voting web sites are required further.

REFERENCES


Daeseon Choi is a member of the research group of the “digital identity research team” of ETRI. His major filed of interest lie in the security mechanisms in the distributed environments. He received his diploma in computer science from the POSTECH, Korea in 1997. Since then he has worked on research projects at ETRI and continuously conducted numerous projects on national and international level.

Seunghun Jin is a manager of the research group of the “digital identity research team” of ETRI. His major filed of interest lie in the digital identity management, PKI, PMI, and authentication/authorization. He received his diploma in computer science from the Soongsil University, Korea in 1995. In 2004 he received his PhD in computer science for a national PKI development. He has worked several projects in commerce. Since the 1999 he has joined on research projects at ETRI and continuously conducted numerous projects on national and international level.

Hyunsoo Yoon is a professor of EECS Dept, KAIST. His major filed of interest lie in the mobile adhoc networking, wireless sensor networking, and multimedia virtual network. He received his PhD in computer science from the Ohio State Univ. in 1988. He is member of IEEE Computer Society and Communication Society. He is also member of ACM SIGARCH and SIGCOMM.