Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 9, September 2015, pg.364 – 367

SURVEY ARTICLE

Survey of OpenID Authentication Framework

Prof. Hitesh C. Patel

Assistant Prof., Information Technology Dept., KITRC, Kalol
hiteshldit@gmail.com

Abstract: - In Today's world, Social networking websites are more popular. There are many web applications or web sites available on the internet so users have multiple accounts to log on the websites to access web service. Most of websites are rely on username and password pair because this method is easy and small for users and administrators of those sites. But Using OpenID, we can easily access service through different provider's username and password like Gmail/Yahoo and many more. There is no procedure for registration. OpenID is Most Popular as an Open Source Identity Provider.

Keywords— OPENID

I. INTRODUCTION

There are many web applications available on the internet so users have multiple accounts to log on the websites to access web service. Most of websites are rely on username and password pair because this method is easy and small for users and administrators of those sites. Users have multiple accounts for different websites. So, users must know that usernames and password for that accounts. But it is a challenge for a particular user to remember different websites' usernames and password.

To make it simple, the use of web applications, user tends to choose one single pair of username and password for all the applications. In order to solve this problem, several protocols or standards are suggested to improve on this situation. For example, SAML [1], OpenID [2], CardSpace [3], OAuth [4] etc. Among the Above, OpenID is most popular today and can be practically deployed. In today's world, number of OpenID user is quickly increasing due to its simplicity. OpenID is an open, decentralized, free framework for user-centric digital identity [2]. It is a single sign on protocol that can be solve the above problem using a single pair of UserID and password for different websites which supports OpenID. OpenID is supported by several larger websites. Users are login into website using their unique userID, i. e. their Username and their userID is Open to all the web application on the internet. The password is centrally managed by OpenID provider. So openID provider is taking the most responsibility for user's information security. But these ways is not secure because openID provider is attacked in some way, there is a disaster for users.

This paper is organized as follows. Section 1 presents introduction of normal authentication process. Section 2 shows the OpenID Authentication Mechanism. Section 3 presents survey of Authentication Mechanism using OpenID. Section 4 describe conclusion.

II. OPENID

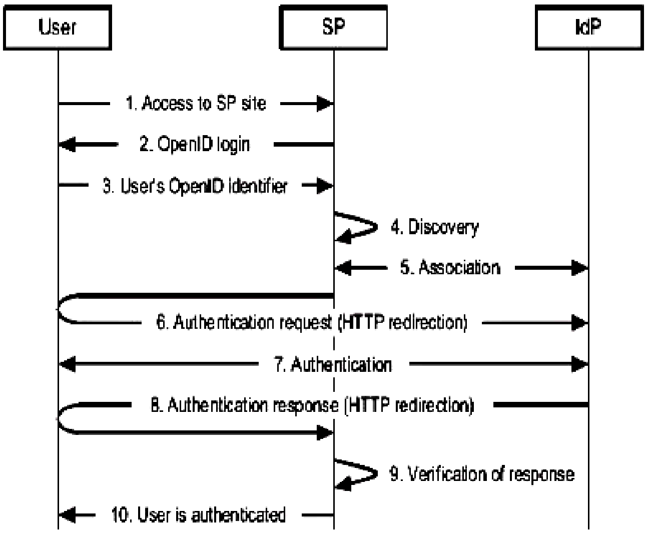
User
SP
IdP
1. Access to SP site
2. OpenID login
3. User's OpenID identifier
4. Discovery
5. Association
6. Authentication request (HTTP redirection)
7. Authentication
8. Authentication response (HTTP redirection)
9. Verification of response
10. User is authenticated

Figure 1. OpenID Authentication Flow [5]

OpenID mechanism is a decentralized authentication scheme for the SSO (Single Sign On) mechanism [5].OpenID users can choose a trustworthy OpenID server to register their OpenID. They are identified by a URL like: http://yourname.openidserver.com. In OpenID mechanism, three parties are involved: the OpenID provider (OP), the service provider which is also called Relying Party (RP) and the user. We assume that the OP and the RP trust each other in advance; OP has a trusted list of RPs. In OpenID mechanism, users only need to have a pair of identity and password. The User then submits his OpenID Identifier. An OpenID authentication flow describe below in figure 1 [5].

The Complete flow of OpenID authentication process describes as below:

A. The user requests access to a service or resource at the SP site. At this moment, we assume that the user is not authenticated.

B. The SP requires the authentication of the user and asks for his OpenID identifier. In order to do so, the SP shows the user an OpenID login page, where he can supply an OpenID identifier.

C. The user provides an OpenID identifier. He may have several identifiers, and he can choose which one to use.

D. The SP performs a discovery process using the supplied identifier to locate the IDP of the user.

E. The SP and the IdP perform an association process, that is, they generate a shared secret through a Diffie-Hellman key exchange. This shared secret will be used to verify subsequent communications.

F. The SP constructs an authentication request and redirects the user to the IdP site through an HTTP redirection. We will assume that the Attribute Exchange extension is used, so the SP also includes a petition for a set of attributes into the authentication request.

G. User gets authenticated by the IdP, for example, by providing his credentials. OpenID does not define a method of authentication, but password-based methods are the most common ones.

H. The IdP constructs an authentication response, which contains an assertion about the result of the authentication. In case the SP asks for attributes, the IdP also includes their values. Additionally, the IdP signs the request. The user is then redirected back to the SP site in order to continue with the authentication process.

I. The SP verifies the authentication response and reads the attribute values included within. The user gets authenticated at the SP site and is able to access to the requested service.

III.SURVEY OF AUTHENTICATION MECHANISM USING OPENID

The original OpenID authentication protocol was developed in May 2005 by Brad Fitzpatrick, creator of popular community website LiveJournal, while working at Six Apart [6]. Initially referred to as Yadis (an acronym for "Yet another distributed identity system"), it was named OpenID after the openid.net domain name was given to Six Apart to use for the project. OpenID support was soon implemented on LiveJournal and fellow LiveJournal engine community DeadJournal for blog post comments and quickly gained attention in the digital identity community. Web developer JanRain was an early supporter of OpenID, providing OpenID software libraries and expanding its business around OpenID-based services [6].

Late in 2006, a ZDNet opinion piece made the case for OpenID to users, web site operators and entrepreneurs [7]. On January 31, 2007, Symantec announced support for OpenID in its Identity Initiative products and services [8]. In mid-January 2008, Yahoo! announced initial OpenID 2.0 support, both as a provider and as a relying party, releasing the provider service by the end of the month [9]. In January 2009, PayPal joined the OpenID Foundation as a corporate member, followed shortly by Facebook in February [10]. In March 2009, MySpace launched their previously announced OpenID provider service, enabling all MySpace users to use their MySpace URL as an OpenID. In May, 2009 Facebook launched their relying party functionality [11].

In 2010, open Identity Management Framework also used for Mashup. Mashup have emerged as a Web 2.0 phenomenon, connecting disjoint applications together to provide unified services [12]. In 2011, OpenID Identity Management Framework is also used in Openstack Cloud Computing for Authentication purpose [13].

In 2012, OpenID Identity Management Framework used with the Combination of Encryption/decryption process like proxy re-encryption with OpenID to enhance privacy in cloud-based identity services [5].

But OpenID is vulnerable to phishing Attack so some extra authentication mechanism is needed to improve performance of OpenID in term of security.

Today, OpenID identity framework used with the OAuth web Authorization protocol. OAuth, a new protocol for establishing identity management standards across services, provides an alternative to sharing our usernames and passwords, and exposing ourselves to attacks on our online data and identities [14].

IV. CONCLUSIONS

OpenID is Open Source Identity framework and it is used for authentication fastly. OpenID is also reducing the registration process for authentication. But some extra functionality needed which can improve security of OpenID Authentication framework.

REFERENCES

[1] S. Cantor, et. al. (ed.), Assertion and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15March 2005.

[2] OpenID Web site, http://www.openid.net.

[3] Microsoft, Windows CardSpace, online: http://en.wikipedia.org/wiki/Windows_CardSpace.

[4] http://oauth.net/about/.

[5] DavidNunez, Isaac Agudo, and Javier Lopez, Integrating OpenID with proxy re-encryption to enhance privacy in cloud-based identity services, IEEE 4th International Conference on Cloud Computing Technology and Science, 2012.

[6] http://en.wikipedia.org/wiki/OpenID.

[7] http://www.zdnet.com/blog/digitalid/the-case-for-openid/78

[8] *http://www.symantec.com/about/news/release/article.jsp?prid=20070131_01*

[9] http://web.archive.org/web/20080304014817/http://biz.yahoo.com/bw/080117/20080117005332.html

[10] http://developers.facebook.com/blog/post/2009/05/18/facebook-supports-openid-for-automatic-login/

[11] http://www.pocket-lint.com/news/95585-facebook-accepting-google-login-openid

[12] *Ding Chu, Qing Liao and Jingling Zhao, Open Identity Management Framework for Mashup, IEEE, 2010.*

[13] Rasib Hassan Khan, Jukka Ylitalot and Abu ShohelAhmed, OpenID Authentication As A Service in OpenStack, IEEE, 2012.

[14] Barry Leiba, OAuth Web Authorization Protocol, Huawei Technologies, barryleiba@computer.org