International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 5 Issue 5, May-2016

A Novel Method for Open Id

Pooja[1], Ashok Kaushik[2]

[1]PG Student, Dept of CSE, BITS Bhiwani, Haryana
[2]Assistant Professor, Dept of CSE, BITS Bhiwani, Haryana

ABSTRACT

In today's world, digital identity of a person is important for accessing online services. At present, most online service providers maintain their own identity management systems. This approach requires the user to register and authenticate separately for each online services. Furthermore, this approach spreads the user's private information to different services and locations which can impact the user's privacy. To overcome these problems, user centric federated identity management solutions are introduced which enable the user's control over his identity information and use the same user identity for many online services. OpenID is one of the most promising user centric federated identity management solutions. OpenID allows the user to access several online services (i.e., web sites) with a single identifier and control his identity information. Furthermore, it reduces the user's burden to remember online service specific username and password. OpenID provides an easy way for services to identify the user.

However this facility users information more vulnerable, since there are several security related issues. Hence in this work a advance anti phishing method is proposed it is neither system nor browser specific .In the following work existing functionality of open id and various security threads especially phishing attack have been studied. The proposed method is easy to understand and the deploy on the existing open id provider without any additional overhead. The feasibility of proposed method has also been compared with the existing solution of open id.

Keywords: OpenId, access, issue, web. Interface.

INTRODUCTION

With the growth of web, the management of username/password pairs becomes difficult. User does not want to register himself/herself for every website he/she wants to use. To resolve this issue OpenID came into picture. OpenID has a number of security issues. To resolve these issues some solutions have been proposed. Phishing is the big flaw in OpenID. A phished page is the mimicked page of original one. To solve this issue a solution is proposed in this work. This chapter provides the basic information about OpenID, starting from OpenID and its security issues towards phishing problem of OpenID. Further it provides the various objectives, scope, thesis contribution and organization of report in to various chapters.

PROBLEM BACKGROUND

In today's world, digital identity of a person is important for accessing online services. At present, most online service providers maintain their own identity management systems. This approach requires the user to register and authenticate separately for each online services. Furthermore, this approach spreads the user's private information to different services and locations which can impact the user's privacy. To overcome these problems, user centric federated identity management solutions are introduced which enable the user's control over his identity information and use the same user identity for many online services. OpenID is one of the most promising user centric federated identity management solutions. OpenID allows the user to access several online services (i.e., web sites) with a single identifier and control his identity information. Furthermore, it reduces the user's burden to remember online service specific username and password. OpenID provides an easy way for services to identify the user.

The OpenID protocol implements a Single Sign-On (SSO) solution for the Internet to help reducing the number of authentication credentials. Single sign-on means that users only need to use one set of authentication credentials to authenticate to several service providers. The OpenID protocol consists of two parts, the **R**elying **P**arty (RP) and the **O**penID **P**rovider (OP). The Relying Party is an OpenID enabled service that uses OpenID to authenticate the users and the OpenID provider is performing the actual authentication task. This research work evaluates the security issues of OpenID.

SECURITY ISSUES IN OPENID

Several security related issues have been raised against OpenID. The issues listed here aren't just protocol related. They are a combination of protocol shortcomings, browser and deployment practices.

Session Related Attacks: OpenID (or any Web SSO protocol for that matter) facilitates user having several active authenticated sessions. It provides more opportunities for a malicious site to exploit the vulnerabilities of OP and other RPs since the user already has an authenticated session.

- **Privacy:** OpenID provider will know every site you log into using its credentials. There isn't any way in the protocol to hide this information from the OP. Since the OP becomes a central place for all login activity across all sites, a malicious OP can easily track user's activity on the internet.
- **Centralized Risk:** Your OP account is much more valuable to the hackers. They hack once and have access to multiple sites. The more successful an OP gets, the more beneficial it becomes for hackers.
- **Co-relation:** If the user uses the same OpenID identifier at various RP sites, the RP sites can get together and co-relate user's information / activity. If the user has independent logins at various RP sites, this is not possible or at least harder to achieve.
- **Security:** Attacker can enter identifiers that can result in buffer overflow, injection, directory traversal attacks at RP sites.OpenID identifier is simply a URI. When a user enters the identifier at a site, the site has to download the URI and data from an arbitrary host which is extremely risky.
- **Replay attacks:** Many RPs doesn't check for nonce and aren't protected against replay attacks.
- **Recycling:** OP policy of recycling identifiers isn't the same as RP's policy. OP's don't communicate to RPs while recycling an identifier.

Phishing: Phishing is serious security issue in OpenID. In phishing attack a mimicking page acts as the original sign in page. There are two common phishing attacks in the OpenIDsystem:

- Phished OP Page.
- Realm Spoofing

OPENID: OpenID is a safe, faster, and easier way to log in to web sites. It is an open, free protocol which allows user to use a single identifier to login to any OpenID-enabled website. It allows the website to communicate with user's OpenID provider when attempting to verify login. Usermay choose to associate information with OpenID that can be shared with the websites user visits, such as a name or email address. With OpenID, user controls how much of that information is shared with the websites you visit. OpenID is rapidly gaining adoption on the web. With OpenID, user's password is only given to identity provider, and that provider then confirms the identity to the websites user visits. If user uses any of the following services, he already has his OpenID:

AOL	-	openid.aol.com/graphicmist
Blogger	-	graphicmist.blogspot.com
Flickr	-	www.flickr.com/photos/graphicmist
LiveDoor	-	profile.livedoor.com/graphicmist
LiveJournal	-	graphicmist.livejournal.com
SmugMug	-	graphicmist.smugmug.com

High Level View of Openid: OpenID enables an end-user to communicate with a relying party. This communication is done through the exchange of an identifier or OpenID, which is chosen by the end-user to name the end user's identity. An Identity provider provides the OpenID authentication (and possibly other identity services). The exchange is enabled by a User-agent, which is the program (such as a browser) used by the end-user to communicate with the relying party and Open ID provider.

- **Relying Party (RP):** A relying party (RP) is a web site or application that wants to verify the end-user's identifier. Other term for this party is "service provider".
- **OpenID Provider:** An identity provider or OpenID provider (OP) is a service that specializes in registering OpenID identifiers.
- **User:** An end-user is the entity that wants to assert a particular identity.
- **ID Server:** The server on which the OpenID identifier page is located. The ID Server can be same as OpenID Provider (OP).

Communication In Openid Communication in OpenID is performed in a particular data formats and in two ways, direct communication and indirect communication. Data formats and type of communication is described in below section.

- ***Data Formats:*** OpenID uses the following data formats for messages and encoding.
- **Protocol Messages**
- **Key-Value Form Encoding**
  - **HTTP Encoding:**
  - **openid.ns:** Value: http://specs.openid.net/auth/2.0 or or http://openid.net/signon/1.1If this value is absent or set to one of "http://openid.net/signon/1.1" or "http://openid.net/signon/1.0", then this message should be interpreted using OpenID Authentication 1.1 Compatibility mode.
  - **openid.mode:** Value: Specified individually for each message type.

PROPOSED METHOD

The proposed anti-phishing method can be broadly divided into three categories:

1. Acquiring Identifier
2. Discovery
3. Authentication

The Authentication step can be further divided into:

3.1 Authentication Request
3.2 OP Validation Against Phishing
3.3 User Authentication
3.4 Authentication Response
3.5 Authentication Verification

A general schematic diagram of proposed method is shown in Figure 3.1. This diagram explains how information flows between different entities of OpenID protocol.

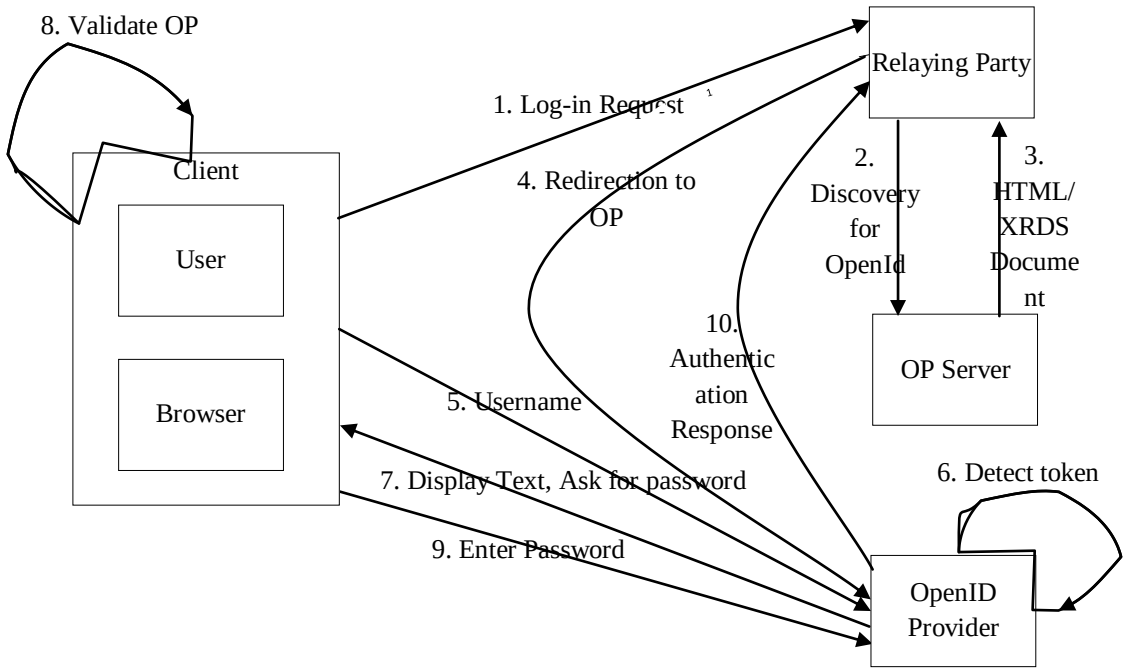

Figure 1: Information flow in OpenID

Acquiring Identifier: The login process starts when the browser visits RP. The user sends a login request to RP as shown in step1 in Figure 3.1. RP requests the end user for his unique OpenID identifier. This identifier is the first bit of information sent from the end-user to the relying party. This request is usually made through an HTML form. Browser can automatically determine that this is an OpenID form because of its attribute named openid_identifier. The OpenID identifiers provided by the user can be of two types. **U**niform **R**esource **I**dentifier (URI) and eXtensible Resource Identifier(XRI). URI is a string of characters used to identify a name or a web resource. The goal of XRI is a standard syntax and discovery format for abstract, structured identifiers that are domain, location, application and transport independent, so they can be shared across any number of domains, directories, and interaction protocols.

Discovery

After normalizing the OpenID identifier supplied by the user, RP gets the HTML/XRDS document from the location of OpenID URI/XRI. This document is retrieved via a process called discovery. RP can perform two types of discovery depending upon the identifier provided by the user. If the document pointed by OpenID is an HTML document, RP will perform *HTML based discovery*, otherwise discovery will be *XRDS based discovery*. In this proposed work, only HTML documents are used for OpenID. The discovery process locates the HTML document located at the OP server as shown in Figure 3.1, step 2. The OP server returns the HTML document to RP. RP extracts two pieces of information from this document:

Address of OP end point 2.OpenID version.

Authentication

After discovery, RP has the sufficient information to communicate with OP. But for the secure communication, RP uses asymmetric encryption technique. So both parties send the data in encrypted form to each other. The authentication process performs in following steps.

- Authentication Request
- OP Validation against Phishing
- User Authentication
- Authentication Response
- Authentication Verification.

IMPLEMENTATION

The user starts by registering at OP.

OPENID PROCESS

The user starts the web browser and enters the name of the site in the browser which he wishes to visit. Here, that site is the RP. The RP URI is *rpserver.com*. This is shown in Figure 2.

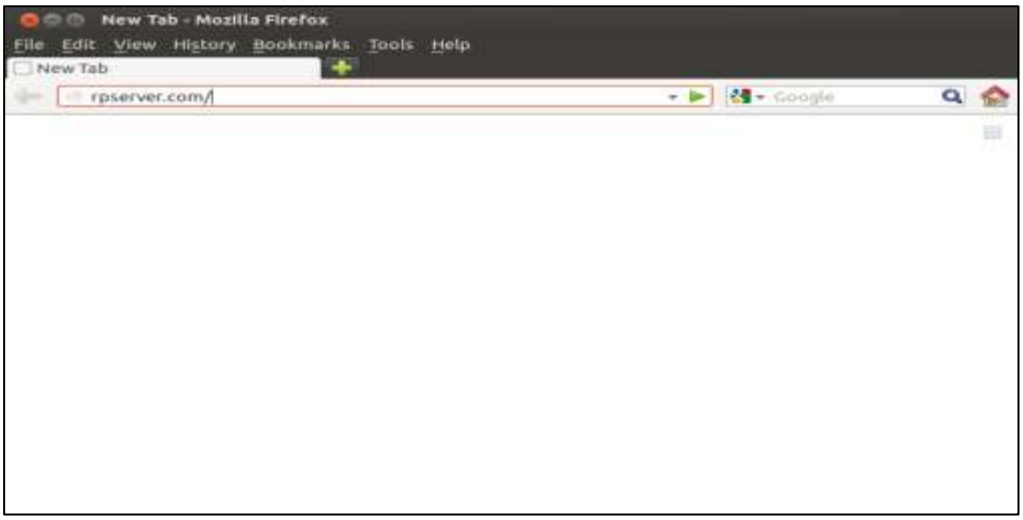

Figure 2 : User entering RP server address in his brows

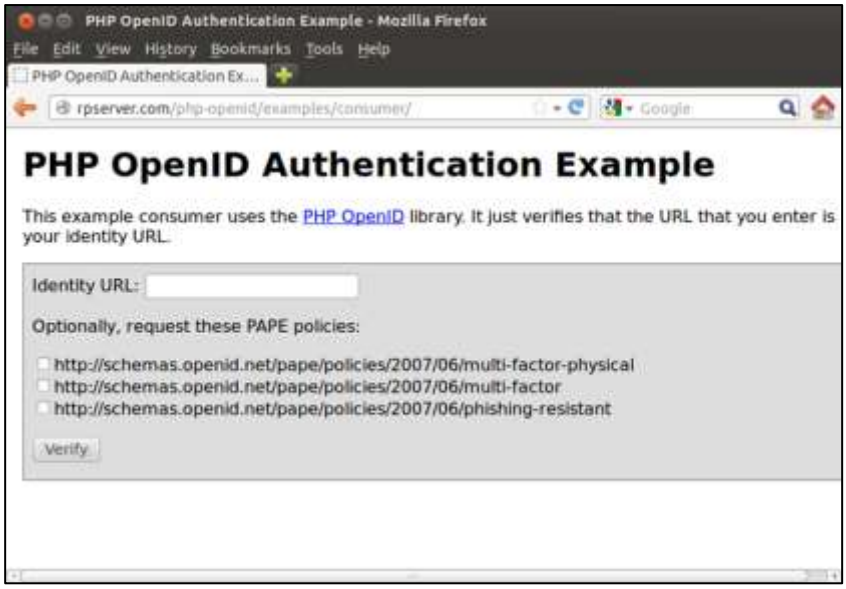

Figure 3: shows the RP website page which is returned to the user.

Figure 4: User enters OpenID URI

After entering the OpenID, the RP performs discovery to retrieve the document pointed by OpenID URI, i.e. *pooja.poojainspiron.com.* From this document, the RP gets the address of OP server. If we check the source of the page at *pooja.poojainspiron.com*., the rel link containing address of OpenID server id found as shown in Figure 5.

The RP now redirects the user to this OP identity server address extracted from the OpenID URI of raghu user, i.e. *pooja.poojainspiron.com.* The user is welcomed by the login page of OP as shown in Figure 5.

Figure 5: Login page of OpenID identitiy server (or OP)

The user enters his/her username at login form as shown in Figure 6

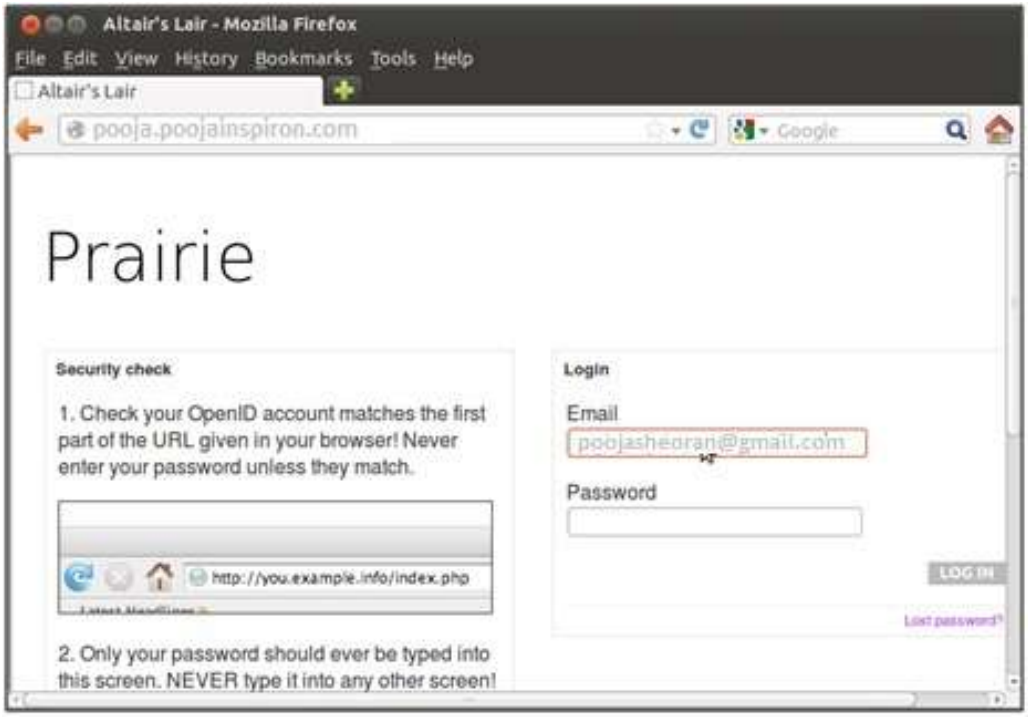

Figure 6: User entering his/her username

The OP checks the security token associated with user account and fetches it to display to the user as shown in Figure 7.

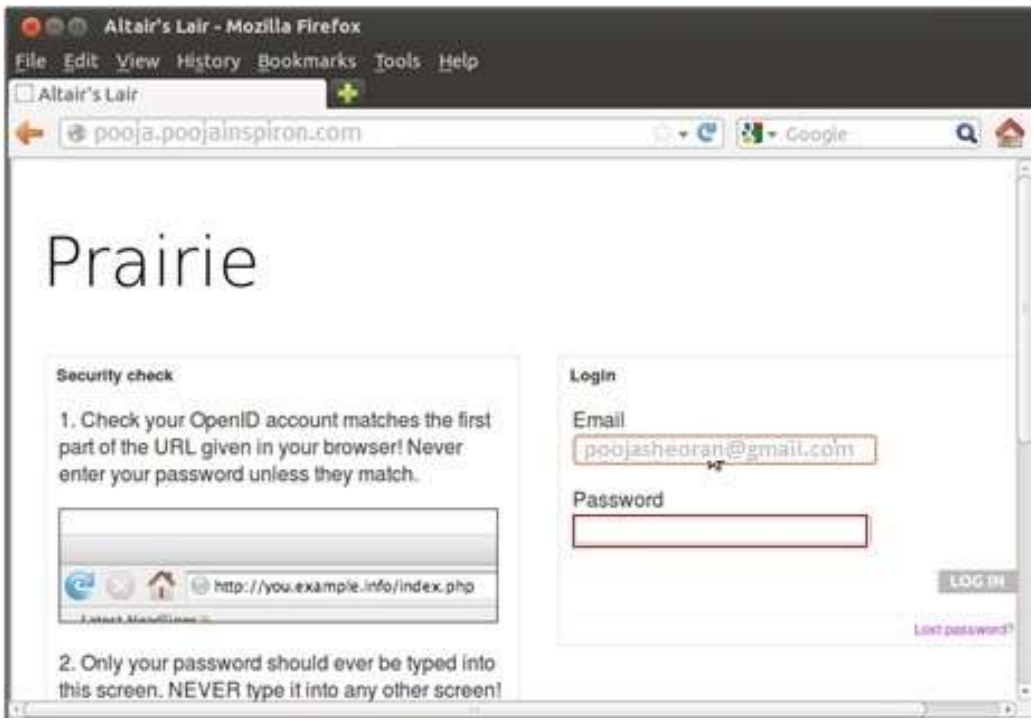

Figure 7: OP shows security token to user

If the user credentials are correct, the user is successfully logged in. OP server informs the user about RP that it is asking for the user's information. The user must confirm to RP if he wants to proceed. This is shown in Figure 8.

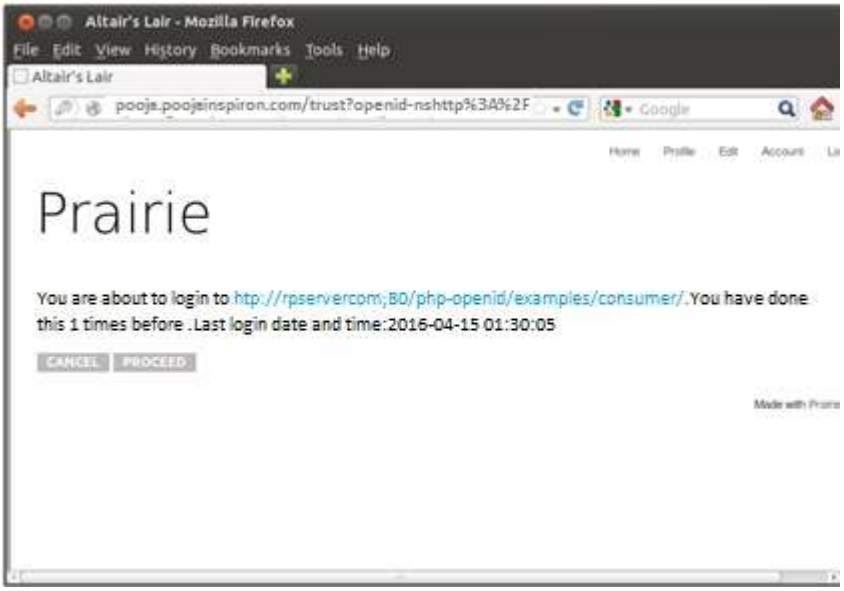

Figure 8: OP asks the user to confirm RP request

If the user chooses to proceed, OP redirects the user back to RP with the information asked as shown in Figure 9

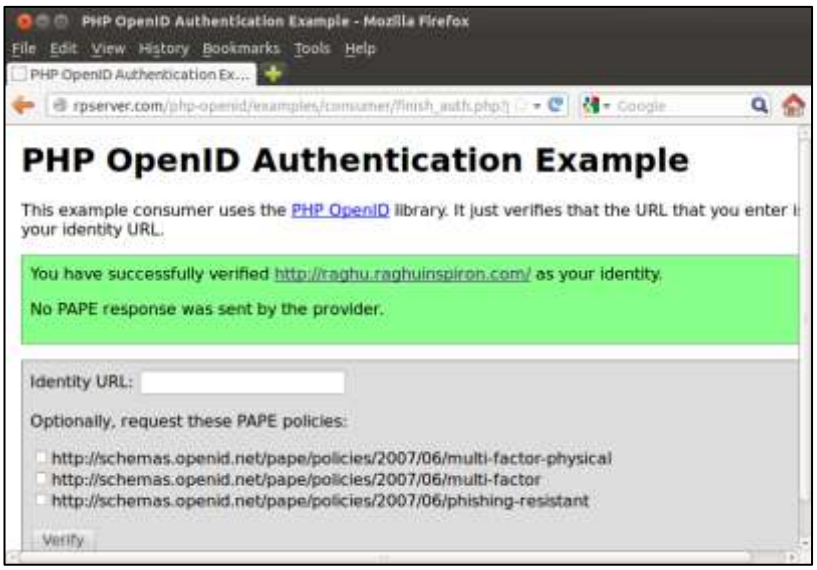

Figure 9: OP redirects the user back to RP

RESULT ANALYSIS

The implementation of proposed method provides an efficient anti-phishing method. It is simple and easy to deploy at existing OPs. From the end user's perspective, the proposed method is very friendly. User does not need to check his email or SMS at login. The existing anti phishing methods have limitations that they are very complex or system/browser specific. But proposed method does not add any complexities to the existing system. All the information about the token is kept at OP, which makes it system or browser independent. The performance of OpenID protocol is not affected by including this method in the existing implementations. Hence it is easily realizable.

The proposed are suggested as a means of anti-phishing in OpenID. To prevent phishing perfectly and authenticate Ops and users at the same time, a security token has been used. Finally, it is thought that anti-phishing methods should be standardized in order to maximize the benefits of OpenID.

CONCLUSION

OpenID is a simple decentralized identity management system. A user can choose from a number of OpenID providers available. If he/she wishes or does not trust an Identity provider, he/she can switch to some other provider or be an Identity provider himself/herself. OpenID is rapidly gaining adoption on the web, with over one billion OpenID

enabled user accounts and over 50,000 websites accepting OpenID for logins. Users may create accounts with their preferred OpenID identity providers, and then use those accounts as the basis for signing on to any website which accepts OpenID authentication. With OpenID, users no longer need to create accounts on every other website and remember passwords for all these different websites. But with all the facilities and ease OpenID provides, it has its own security threats. Among other threats such as session swapping, replay, CSRF (Cross Site Request Forgery), XSS (Cross Site Scripting) etc., phishing is one of the biggest issues with the security of OpenID. In phishing attack, a phished page looking like legitimate page is displayed to the user, which actually is controlled by the attacker. This work proposes and implements a method to prevent phishing in OpenID. Although there are existing anti-phishing methods such as Yahoo sign-in seal, Vidoop's email method, Firefox SeatBelt plugin, VeriSign and IE7's validation certificate, jabber's authentication by messenger or SMS etc, but all of these have some limitations. Yahoo Sign-in Seal stores the seal at user's system; Firefox plugin works for only single instance of Firefox only and VeriSign certificate validation works on Internet Explorer only, so these three are browser or system specific. Vidoop's email method and jabber's authentication increases user's burden of checking email or SMS every time he/she logs in.

The proposed method removes these limitations by using a security token that user selects at the time of registration at OP. This token is displayed at login page when user inputs his login name. As the token is profile specific and chosen by the user, only the user or the OP knows about it.

REFERENCES

[1]. Tapiador A. and Mendo A., "A Survey on OpenIDIdentifiers,"in proceedings of Next Generation Web Services Practices (NWeSP), 2011 7th International Conference, pp. 357-362, 2011.
[2]. Bellamy-McIntyre J.,Luterroth C. and Weber G., "A Model-Based Analysis of Single Sign-On Authentication,"in proceedings of Enterprise Distributed Object Computing Conference (EDOC), 2011,pp. 129-138, 2011.
[3]. Hyun-Kyung Oh andSeung-Hun Jin,"The Security Limitations of SSO in OpenID," in proceedings ofAdvanced Communication Technology, 2008. ICACT 2008. 10th International Conference,pp.1608 – 1611, Feb. 2008
[4]. Jae-Hwe You and Moon-Seog Jun, "A Mechanism to Prevent RP Phishing in OpenID System"in proceedings of Computer and Information Science (ICIS), 2010 IEEE/ACIS 9th International Conference, pp. 876-880, Aug. 2010.
[5]. Xiangwu Ding andJunyin Wei,"A Scheme for Confidentiality Protection of OpenID Authentication Mechanism," in proceedings of International Conference on Computational Intelligence and Security,pp. 310-314, 2010.
[6]. Maler. E and Reed. D. "The Venn of Identity: Options and Issues in Federated Identity Management, Security & Privacy," in proceedings of IEEE, vol. 6, no. 2. pp. 16-23, 2008.
[7]. Huping Wang, Chunxiao Fan, Shuai Yang, JunweiZou andXiaoying Zhang,"A New Secure OpenID Authentication Mechanism Using One-Time Password (OTP)", in proceedings ofWireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference, pp. 1-4, 2011
[8]. Riesch, P.J, Xiaojiang Du,"Audit Based Privacy Preservation for the OpenIDAuthentication Protocol," in proceedings of IEEE Conference on Technologies, pp. 348-352, Nov. 2012.
[9]. Sun S-T, Hawkey K andBeznosov K "Systematically Breaking and Fixing OpenIDSecurity: Formal Analysis, Semi-Automated Empirical Evaluation, and Practical Countermeasures," in proceedings of Computers & Security, vol. 31 no. 4, pp.465-483,Jun 2012.
[10]. Junyin Wei,Mingxi Zhang,Xiangwu Ding and Ying Wang, "Research on Multi-Level Security Framework for OpenID" in proceedings of Electronic Commerce and Security (ISECS), 2010 Third International Symposium, pp. 393-397,July 2010.
[11]. Hyun-kyung Oh andSeung-hun Jin,"The Analysis of SSO in OpenID," in proceedings of APIS, pp.15-18, 2007.
[12]. Hwan Jin Lee, InKyung Jeun,Kilsoo Chun andJunghwan Song "A New Anti-phishing Method in OpenID" in proceedings of Emerging Security Information, Systems and Technologies, SECURWARE '08., pp.243-247, 2008.
[13]. Kazunari M., Yoshio K. and Keiichi I. "Innovative Mobile and Internet Services in a Ubiquitous Computing (IMIS)," Fifth International Conference, pp. 612-617, 2011.
[14]. Sun S-T, Hawkey K andBeznosov K. "OpenIDEmail Enabled Browser Towards Fixing the Broken Web Single Sign-on Triangle,"in proceedings of the 6th ACM, pp.49-58,2010.
[15]. Volchkov,"Revisiting Single Sign-on: A Pragmatic Approach in a New Context," in proceedings of IEEE, pp. 39-45, 2001.
[16]. Maler. E and Reed. D.,"The Venn of Identity: Options and Issues in Federated Identity Management, Security & Privacy," in proceedings of IEEE, vol. 6,no. 2. pp. 16-23, 2008.
[17]. Khan R.H., Ylitalo J. and Ahmed A.S., "OpenIDAuthentication as a Service in OpenStack," in proceedings of Information Assurance and Security (IAS), 2011 7th International Conference, pp.372-377, 2011
[18]. D. E. Bell and L. J. LaPadula,"Secure computer systems: A mathematical model" in proceedings of The MITRE Corporation, Bedford, Massachussatts: Technical Report,pp. 74-244, 1973.
[19]. D. Recordon and D. Reed, "OpenID 2.0: A Platform for User Centric Identity Management," in proceedings of the second ACM workshop on Digital identity management (DIM '06). New York, NY, USA: ACM, 2006, pp. 11–16.
[20]. Jennifer G Steiner, Clifford Neuman, and Jeffrey I Schiller, "Kerberos: An Authentication Service for Open Network Systems," in proceedings of theWinter 1988 Usenix Conference, pp. 191-201, 1988.