International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 4, April 2013 **ISSN 2319 - 4847**

Enhanced OpenID Protocol in Identity Management

Ronak R. Patel[1], Bhavesh Oza[2]

[1]PG Student, Department of Computer Engg, L.D.College of Engineering, Gujarat Technological University, Ahmedabad

[2]Associate Professor, L.D.College of Engineering, Gujarat Technological University, Ahmedabad

ABSTRACT

Identity management in multilayered architecture has had many hurdles. Not only can it be extremely time consuming to get everything set up correctly, it can also be expensive. Identity management is the process by which user identities are defined and managed in enterprise environment. This paper demonstrates how identity information sent within the OpenID protocol can be manipulated, due to an improper verification of OpenID assertions and no integrity protection of the authentication request.

Keywords: Identity Management, Relaying Party, Identity Provider, User Agent, Privacy.

1. INTRODUCTION

A. Identity Management

Identity management is the process by which user identities are defined and managed in enterprise environment. Identity management (IdM) describes the management of individual identifiers, their authentication, authorization, and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks. Identity management is a relatively new term that means different things to different people. Frequently, IT professionals have tended to pigeonhole its meaning into certain identity and security related problems that they are currently faced with. For example, Identity Management has been perceived to be a synonym for single sign-on, password synchronization, meta-directory, web single sign-on, role-based entitlements, and similar ¬ customers, trading partners, or Web services, as well as users inside an organization. In addition, an identity management system can manage network entities other than users, such as devices, processes, and applications.

B. Basic Objectives

(1) Improve Administration
(2) Improve Security
(3) Reduce Complexity
(4) Increase Efficiency
(5) Improve Compliance
(6) Leverage Standards
(7) Position for the Future
(8) Enable Integration

C. Benefits

(1) Improved quality of service to the users.
(2) Faster processing of requests.
(3) Automation speeds for the processing of requests, freeing security administrators to spend time on other important activities.
(4) Implementation of the common processes across multiple accounts will standardize and simplify procedures, reducing mistakes and cost.
(5) Improved enterprise security with complete visibility into user access privileges.
(6) Provisioning of client accounts takes minutes rather than days to build.
(7) Eliminated or reduced duplicate user IDs.

D. IDM Issues and Problems:

Administration

• No centralized user administration process.

- Multiple teams are involved in the user administration activities.
- Increasing overhead in administration of identities
- Administrators spend a lot of time performing routine admin tasks that can be automated
- Different administrators often assign different IDs to the same person. This makes it difficult to track activity back to a single source and confuses the customer [1].

Security

- Potential security risks
- Accounts are created with unauthorized system access rights.
- Security risks occur when frustrated or overburdened admin staffs may take shortcuts, terminations may not be done as soon as required or permissions granted may be in excess of what is really needed.

Complexity

- The users of the system are located worldwide and can be customers, employees, temporary workers, contractors and external suppliers.
- Multiple authentication requirements for applications
- Account creation/deletion in repositories is performed by multiple groups
- Many systems and applications have different business owners, platforms, administrative tools, and system administrators, leading to slow performance, delayed or unreliable terminations and higher administration costs[1].

Inefficiency

- A high number of calls are made to the support center for user provisioning activities including password resets.
- Terminating employee accounts is a manual process
- The process for business unit managers and application owners to sign off on the privileges of the users is cumbersome and time consuming.
- Redundant identity information
- Users wait longer than necessary to obtain IDs
- Authorizations needed to process a request often slow the process of account creation or update and leads to errors and mistakes.

Compliance

- Untimely response to regulations

E. Identity Management Terminology:-

The following list defines some important identity management terms and concepts[2]:

- Authentication: The process of verifying the identity claimed by an entity based on its credentials.
- Authorization: The process of establishing a specific entitlement that is consistent with authorization policies.
- Authorization policies: Declarations that define entitlements of a security principal and any constraints related to that entitlement.
- Entitlements: The actions an entity in a network is allowed to perform and the resources to which it is allowed access.
- Identity: The set of attributes that uniquely identifies a security principal. A security principal can have many different accounts that it uses to access various applications in the network. These accounts can be identified by these applications using different attributes of this entity. For example, a user can be known in the e-mail service by an e-mail ID, whereas that same user can be known in the human resource application by an employee number. The global set of such attributes constitutes the identity of the entity.
- Identity administration: The act of managing information associated with the identity of a security principal. The information can be used by the identity management infrastructure itself to determine administrative privileges.
- Metadata repository: A database used to hold metadata, including identity information.
- Provisioning: Notification of applications whenever changes are applied to company Internet Directory.
- Realm: A collection of identities and associated policies which is typically used when enterprises want to isolate user populations and enforce different identity management policies for each population.
- Security principals: The subjects of authorization policies, such as users, user groups, and roles. A security principal can be a human or any application entity with an identity in the network and credentials to assert the identity.

2. OPENID IDENTITY MANAGEMENT PROTOCOL

OpenID Roles

- The User is an entity wanting to authenticate against a Relying Party with his digital identity.
- The Identifier is generally a url, representing the User. It points to a resource, which holds information such as the User's OpenID Provider url, version of OpenID which the OpenID Provider is compatible with etc[3].

- The Relying Party is an entity accepting an assertion from an OpenID Provider, representing a digital identity of a specific User.
- The OpenID Provider or Identity Provider (interchangeable terms) is responsible for authenticating the User against a Relying Party, therefore it is the trusted third party on which the User as well as the Relying Party rely. In order to do so, the User must authenticate against the OpenID Provider first and so prove his digital identity. This identity is then used to sign-in the User at the Relying Party by accepting a security assertion from the OpenID Provider[4].

A typical OpenID Authentication 2.0 Protocol flow Shown below figure[5].

1. OpenID Authentication 2.0 Protocol is initiated by the User by requesting the Relying Party's site.
2. The Relying Party responds with its login page presenting an input field for an Identifier.
3. The User enters his Identifier and submits the login page form, i.e. requests OpenID Authentication 2.0 Protocol.
4. The Relying Party performs discovery upon the received Identifier i.e. retrieves the data resource held at an Identifier's url and
5. subsequently receives metadata representing the User and his OpenID Provider.
6. Based upon metadata from the previous step, the Relying Party requests an association from the OpenID Provider, i.e. requests to exchange a shared secret.
7. The OpenID Provider responds with a shared key, which is encrypted (either using HTTPS as transport protocol or using Die-Hellman Key Exchange).
8. The Relying Party then redirects the User to the OpenID Provider by sending a HTTP(S) response with the redirect header pointing to the OpenID Provider's endpoint.
9. The User is presented with a login form at the OpenID Provider.
10. The User fills out the login form and submits it, hence authenticating against the OpenID Provider.

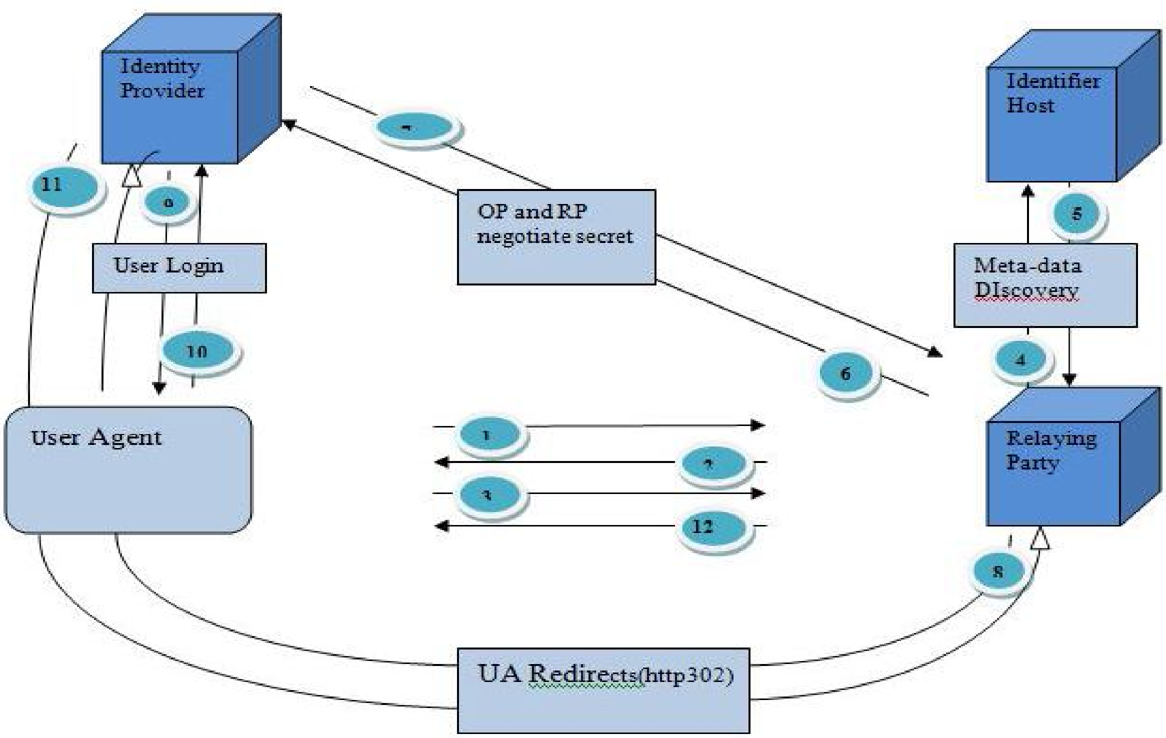

Figure 1 OpenID Protocol Flow[6]

11. The OpenID Provider verifies the User's credentials and, if these are valid, redirects the User to the Relying Party along with the authentication result (MAC-protected by the previously established shared key). Again, this is done using a HTTP(S) redirect with the 'Location:' header pointing to the Relying Party's endpoint. The assertion in this request to the Relying Party indicates the login success from the OpenID Provider and the MAC ensures the integrity of the response.
12. According to the OpenID Provider's response, the User is either authenticated against the Relying Party or presented with an adequate error message.

3. EXTENDED OPENID

A. Sequence Diagram

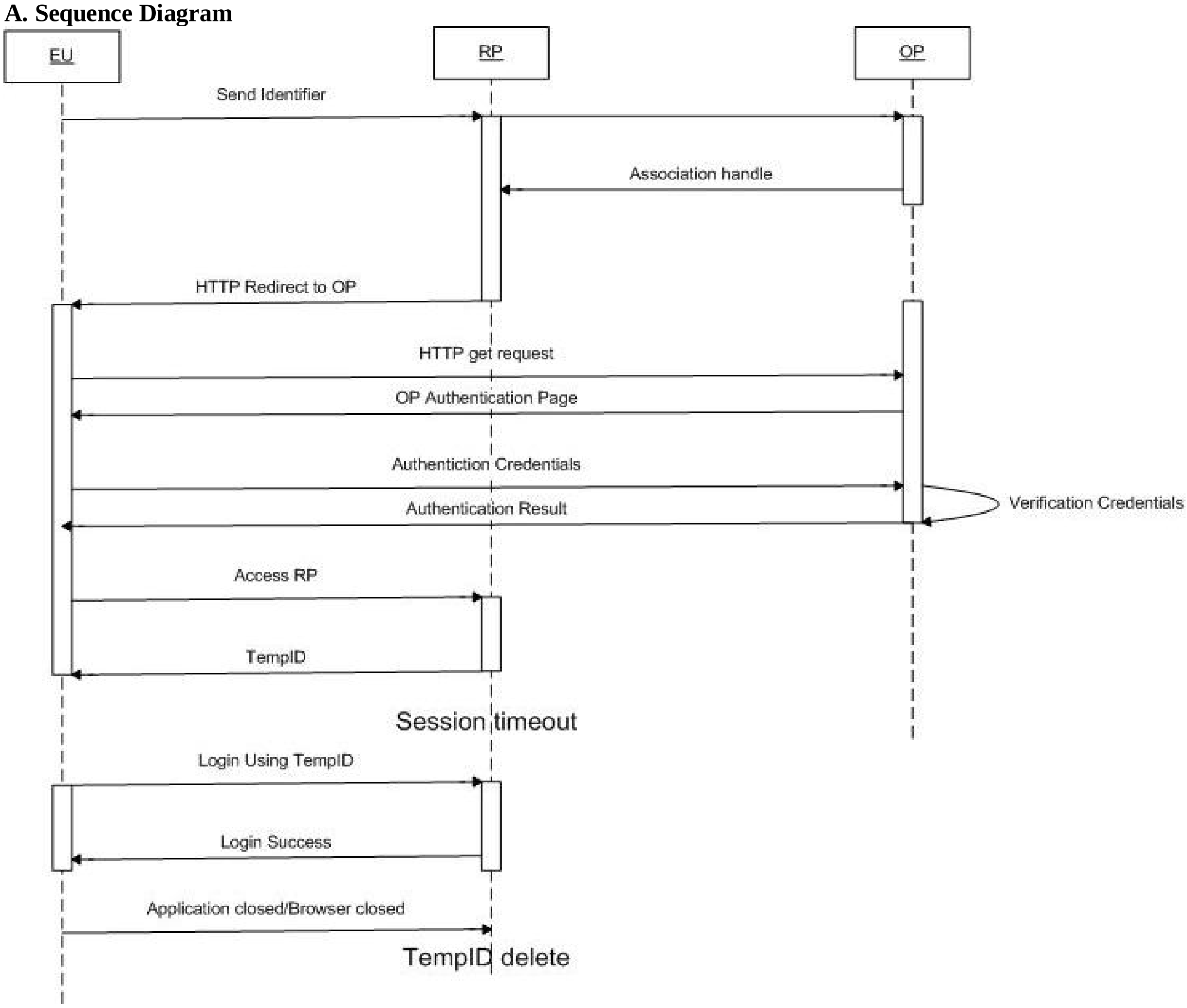

Figure 2 Extended OpenID Protocol

B. Event Scenario for Extended OpenID protocol

1. User send request to RP for identification.
2. RP request association from OP.
3. OP responds with a shared key, which is encrypted.
4. RP redirects the user to OP.
5. OP presents its login form to user for Authentication detail.
6. Users fills the authentication details and submit.
7. OP verifies user's authentication credentials.
8. OP response to RP with username.
9. Using OP's response to RP, the user either authenticated against RP or presented with error message.
10. If authentication success to the OP, user redirect to RP using assertion message from OP.
11. User logged in and service can be provided. At that time RP generate TempID as a password and send to users.
12. So when session timeout, user login again using that username and TempID Which is provided by RP.
13. That TempID is used only upto browser closed or application closed. And valid for only 24hours.

4. CONCLUSION

We have provided a description and analysis of the OpenID Single Sign-On protocol and its extensions. The model of OpenID seems to be a suitable Single Sign-On solution for the Internet of today. In the OpenID protocol there is a problem with the session so we provide the extended protocol in which we login at the relaying party without redirected to Identity Provider again after session timeout. It has remarkable usability properties and the concept of extensions makes it very flexible.

5. ACKNOWLEDGEMENT

Ronak R. Patel would like to thank to my thesis guide Prof. Bhavesh Oza for his great effort and instructive comments in this paper work. Lastly, I wish to thank to all those who helped me during the lifetime of my research work.

References

[1] Mark Dixons, Discovering Identity, https://blogs.oracle.com/identity/entry/identity_problems
[2] Oracle Identity Management Concepts and Architecture, http://docs.oracle.com/cd/B15904_01/manage.1012/b14084/concepts.htm
[3] OpenID Foundation. http://openid.net/
[4]Alexander Lidholm, "Security Evaulation of OpenID Protocol", Sweden-2009
[5] Pavol Sovis, Florian Kohlar, "Security Analysis of OpenID", Germany.
[6]Ronak Patel,Bhavesh Oza,"A comparative study of identity management protocols",cocss-2013.

Author

Ronak R. Patel, pursuing his Master Degree in Computer Science & Technology from Gujarat Technological University (L D College of Engg., Ahmedabad) as a GATE candidate, received his Bachelor Degree in Information Technology from S.P.B. Patel Engineering College, Mehsana From HNGU in 2011.