ISSN:0975-9646

Single-Sign on Using Social Networking Sites.

K.Naveen
Bapatla Engineering College, Bapatla,
Andhra Pradesh, India

Abstract:-This paper describes the best of using single sign on (SSO) using social networking sites. The practice of implementing traditional username/password authentication on the Internet suffers from a number of issues that reduce its efficacy, increase costs, and significantly increase risk for an organization. Fortunately by leveraging third-party Authentication through social login, in which existing identities from social networks like Facebook, Google, and Twitter are used to register and sign in to other sites. Companies can mitigate risks of theft of passwords, reduce costs, and improve new customer conversion rates.

Keywords: SSO, third party authentication

1 INTRODUCTION:-

With the explosion of web2.0 technology, the number of individual sites requiring registration has dramatically increased and it is becoming apparent that the current authentication situation is unsustainable .To deal with the dozens of individual logins and passwords required by different sites, users are being forced to write down their logins or reuse the same username and password for every website. This is clearly undesirable it creates multiple points of attacks on the internet today. In order to improve user experience service providers like Google, Yahoo and others have come together to specify methods to allow users to share their identity among different services in a secure manner without the risk of revealing actual passwords or any confidential information to other services. In enterprise environment this is done by SSO system usually provided by a commercial vendor and by integrating all services inside enterprise to use the system. On the internet an open source standard called OpenId has adopted as main feature of SSO and its becoming more and more popular. Today leading tech companies like Google, Facebook, Yahoo, PayPal all offer SSO services. These services work through the interaction of mainly three parties: the user, the identity provider (IDP) and relying parties which act as service providers (SP).

In order to avoid leaking of private data to non-authorised parties, a trust relation between user and application is required. In this paper we take a look at how this relationship is created to ensure that private data is passed to only authorized parties or sites.

Social networking has been a catalyst for making online identity portable and interoperable. Before social networks, users had no alternative to filling out registration forms when signing up for an account at a website. But now, in the social age, expecting users to once again re-enter their relevant identity data has become impractical, maybe even presumptuous. Facebook, Twitter, and Google offer authentication APIs that make it easy for users to sign in to other websites using an existing profile. By leveraging these APIs, websites can create a personalized experience without requiring the user to register a username, password, and profile data.Keywords: OpenID, Identity Management, IDP, SP.

2 SINGLE SIGN ON:-

Amount of web application is growing rapidly. New services are released on internet all the time and more and more application are used with regular web browsers .Usually each of these application require user to authenticate into them separately forcing people to remember credentials separately to each application. Each application has separate database and user management logic.

In order to reduce cost that are required to maintain the user information and also to ease the usage of these applications, SSO concepts comes handy and very useful. This concept is used by using Security Assertion Markup Language (SAML) which has become a standard protocol for exchange of key information between identity providers (IDP) and service provider (SP).SAML is xml based framework designed to pass identity information between different parties in a secure manner. It has been designed as a flexible and extendable framework based on xml messages.

SSO stands for single sign-on and its simplest form means a way where user can access several applications using centrally managed account information and performing authentication only once. Typically SSO consists of services that users are accessing called service provider (SP) and identity provider (IDP).When service provider needs to authenticate user, it delegates to identity provider that performs the actual authentication of the user usually using username/password with some extra security mechanisms. After IDP has authenticated the user, it provides information back to SP which can then proceed and provide services to the user.

Along with user identification, the IDP or SP can query attributes for the specific identity. Typically these information is about user or information about different roles. Based on these attributes the SP can perform actual authorization process and restrict or allow access to certain features and information in the service. Even though user accounts are stored in IDP, it is often necessary to store some of user attributes locally in SP. These kind of values are needed in internal queries in SP and requesting them from IDP every time would cause severe decrease in performance.

Single Log-out (SLO) is used in SSO environment to logout users from Service Provider. Usage of SLO guarantees that when user wants to logout, he is also logged out from all SP leaving no unwanted session open between SP and IDP.

3 WEB SINGLE SIGN-ON: BACKGROUND

Several approaches has been proposed to address the problems of single sign-on in different scenarios and one of the successful approach is OpenId for web applications.

3.1 Web Applications Single sign-On: OpenId

OpenId is one of the most successful single sign-on solution which provides framework for deploying flexible and centralized user authentication for web applications. In this the user can choose from variety of identifiers which may be any website or any web based application where he already has an account. In order to sign on to a given web application the user first signs to identity provider of his choice and OpenID exchanges the necessary authentication data between identity provider and the service provider.

In order to transfer authentication information between service provider and identity provider, OpenID relies on a complex mechanisms involving authentication information stored as Cookies in the user machine and background Http requests.

3.2 Web Single sign-on: A view from User

SSO is essential an essential process for identity provider to convince service provider that this user has signed on to the IdP before utilizing the services of SP. Browser needs to present a token to SP issued by IdP to demonstrate that it possess that IdP grants to user.

An SSO process can be described as a sequence of browser relayed messages exchanged between IDP and SP. Typically, an HTTP communication can be thought as sequence of request – response pairs as shown in below fig1.

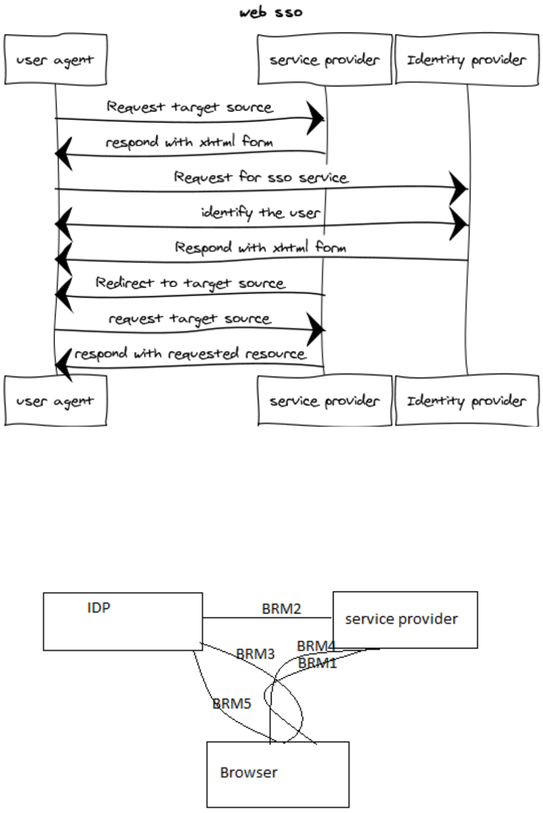

Fig1 single sign on from user's view

Each BRM message describes a step of SSO in which server handler of step x passes the data to server handler of step X+1 with server state piggybacked. The entire process of SSO is started by sending a request from SP to declare its website identity to IDP. More BRM's may occur as needed afterward. The last BRM finally convince the SP that the user details are valid and authenticated by IDP. A BRM can be, for example (1) an HTTP 3xx redirect response (2) a response with a flash or script object to make a request. A BRM can be of a format below tab 1.1

Src=localhost://dst=facebook.com/a/foo.php
Set-Cookie: SessionID=4568784
Arguments pass=**** user=n@yy.com
Cookie: fbs=a91d9 & foo=89dn9d

Tab1.1 An Browser Request Message of having arguments username and password

This BRM represents a localhost as a source server ask the browser to set Cookie sessionID=4568784 for its domain and to send a request to destination URL (dst) facebook.com/a/foo.php, the request containing arguments fbs=a91d9 & foo-89dn9d stored in the browser for domain Facebook.com

3.4 Threat Model

We base our security analysis on a similar threat model that considers attackers with powers to completely controls the communication link between user‘s machine, the identity provider and application/service providers.

Phishing

An attacker may try to lure a user into disclosing his access credentials or accidentally performing unwanted sign-on operations. The attacker may set up spoofed websites and email messages or use other social engineering techniques to compel the user into performing actions that he would not normally carry out.

Network attacks

The attacker has complete control over the user's internet link and overall network, disrupting communication or altering data as he wants. Such attacks can be carried out by adversaries who are naturally in a privileged "gateway" position in the network (which can be achieved, for example, by infecting firewalls). Furthermore, ARP sponge techniques may be used to divert track from the user's machine through the adversary's machine and back to the original destination, actively giving control the user's link.

The adversary is also given complete control over the communication links between the identity provider and the individual service providers.

4 STUDYING SSO SCHEMES ON MAJOR WEBSITES

The study covers popular SSO services on the web (e.g. Google, Facebook, Yahoo and PayPal). In this section we use a tool called HTTP live headers for capturing BRMs.The results show that these prominent web SSO systems contain serious logic flaws that makes it incomplete and realistic for unauthorized party log into customer accounts. We elaborate these vulnerabilities in the below sections

4.1 GoogleID

OpenID is one of the popular standard for single sign-on. It was reported that there were over one and half billion OpenID enabled user accounts and ten million websites using OpenID as of December 2011[xx].

Our Analysis on GoogleID started with raw traffic but it would be time-consuming for human to parse and analyse. Using Http live headers we could obtain the information about the trace. The is shown in the given fig[] in which SP is Odesk.com and IdP is google.com. The details in given below tab 1.2 which are not important to our discussion are marked as [*]

BRM1 src=odesk.com	dst=/oauth/google?cb=google-signup
Arguments:	
visitor_id=IP address.1413870733947145;	
User-Agent [*]: Mozilla/5.0 (Windows NT 6.2; WOW64);	
Cookie: __cfduid=dd0c0682b748b9870c8adb1413870733437;	
Accept-Encoding: gzip, deflate;	
Accept[*]: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8;	
BRM2 src=https://accounts.google.com/o/oauth/auth dst=odesk.com	
Arguments:	
Accept[*]: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8	
Accept-Encoding: gzip, deflate	
Referrer:https://www.odesk.com/signup/createaccount/id/job_5445f52a954158.11090174	
Cookie:PREF=ID=d633b1408572dece:U=87f6a5d5f9699b36:LD=en:TM=1411543500:LM=1411668830	

Tab1.2 Browser Request Message's from source Odesk.com to google.com

We found that BRM3 is the message for providing identity of the user the browser represents. This message contains a single signed token. Among all elements LSOID contains the cookie id for which it validates to IDP's authenticated user. A closer look at them shows that their actual values are propagated from BRM1 which are not under any signature protection. However BRM3 can be controlled adversary through BRM3 there is no guarantee any of the elements that the SP requires the IDP to sign will be signed by the IdP.

It is very common for a website to use a user's email address (e.g., alice@a.com) as his/her username, which is probably why the RP requires email to be signed. The main question to be asked in this scenario is:

Does SP check whether the email element in BRM3 is protected by the IDP's signature?

I turns out that this question indeed points to serious logic flaw in Google Id. But we found that all the elements are secured and signed by the IDP.

4.2 Facebook ID

Authentication on Facebook often goes through Facebook connect, which is part of Facebook platform. We studied the pattern of this SSO scheme.

We performed our automatic analysis on the traces collected from an SSO through Facebook connect. The results are shown in the given table 1.3 .Here IDP is facebook.com and SP is nxs.com. We can see a secret token result, which the browser uses to prove to the RP the user's identity. The secret comes from BRM2 as an argument for the API call *http://!IdP/xd_proxy.php1*. This secret token enables the SP to acquire Alice's information from Facebook and also grant her browser access to her account. Also interesting here is BRM1, in which the SP declares to the IDP its identity (e.g., Nxs) through app_id and provides other arguments. Note that though the element cb in the figure is also labelled as SEC, it was found to be generated by the browser and thus not a secret shared between the RP and the IDP.

All the elements there were only readable so users can not send the values of the elements of their own. Thus there shows no possible threats but still it is vulnerable of showing app_id from IDP.

BRM1: src=SP	Dst=https://!idp/permission.req
Arguments: app_id[BLOB] & cb[sec][bg] &next[URL] { http://!idp/connect/xd_proxy.php?origin[name]&transport[word]	
And other elements:	
BRM2: src=!idp	Dest=http://!idp/xd_proxy.php
Arguments: origin[name] & transport[word] &result[sec] &…..&…	
Other elements	
BRM3: src=!idp	Dst=http://RP/login.php
Arguments: origin[name] & transport[word] & result[sec] &….& and other elements	

Tab1.3 Browser Request Messages from source=Sp and dest facebook.com

5 Conclusion

Single sign-on enables user to login quickly and securely to all their applications, websites and mainframe sessions with just one identity. SAML is relatively a mature standard. Many industrial players support them and many identity products support them. Both the protocols SAML and OpenID were independently analysed and their specifications are documented. One of these standards will arguably dominate the Web SSO scheme.

OpenID has support from all major social networking sites such as AOL, GOOGLE+, Facebook, Pintrest. Having a huge user base in these social sites and it became the strength of the most. While social networking itself has been a driving force for many sites in enabling social sign-in from third-party IDPs, it's becoming increasingly clear that encouraging users to sign in with an account that they already have, rather than registering a new one, can have many security benefits.

REFERENCES

1. http://openid.net/2014/04/01/more-momentum-openid-connect-adoption/
2. http://cafesoft.com/support/security/glossary.html
3. http://odesk.com/freelancer/login
4. http://sso-analyzer.org/tools
5. Brian Kissel. "OpenID 2009 Year in Review," http://openid.net/2009/12/16/openid-2009-year-in-review/
6. OASIS Standard. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, 2005.
7. Birgit Pfitzmann and Michael Waidner. "Analysis of Liberty Single-Sign-on with Enabled Clients," IEEE Internet Computing, 7(6) 2003.
8. Single sign-on Enterprise Security for Web application http://msdn.microsoft.com/en-us/library/ms972971.aspx
9. Single sign-on implementation guide Salesforce.com http://help.salesforce.com/help/pdfs/en/salesforce_single_sign_on

10 .janrain:customer identification management http://www.Janrain.com/