Security Issues of Single Sign on Web Services

Anjali Nair
Dept. of Computer Science
SJCET , Palai
anji.gkn@gmail.com

Arun Madhu
Dept.of computer science
SJCET,Palai
arun99@gmail.com

Dr.Jubilant J Kizhakkethottam
Dept.of computer science
SJCET,Palai
jubilantjob@gmail.com

***Abstract*— Internet plays a main role in our life as our whole life revolves around the internet it become too hard for us to imagine our life without internet. As the use of internet increase the security for all types of data also increases. Early days these securities was provided with the authentication process via password, but now a days use of traditional authentication process is more risky for accessing the requirement of todays distributed user. Single sign on has security and user benefits. It reduces the cost too. SSO allows a user to use a single account to access multiple functions provided within that website. However, security is at greater risk if user are providing data for any of weak website then our secret credentials will be at risk.Many algorithms are used to find out what all flaws are present in web services which helps many companies to improve their services & security.**

Keywords: Single sign on, Authentication, Security issues, BRM Analyzer, NRL Analyzer.

I. INTRODUCTION

Now a days one website is providing us with more than one functionality, for example, user are having a Facebook account then with the help of that single username one can access more than one functionalities. Many leading web technology companies are using this technique. These techniques help users memorize only one password and it reduces the cost too user mainly use it when they are having more than one application to access [2]. It is an authentication, which already exists in the early days, but now a days its usage increased as much new technology comes into existence like cloud computing, etc. This authentication help user to access multiple services by using users profile details of users mentioned in the website.

As usage of service increases problem regarding security also increases as this website is dealing with user secrete credentials then risk of getting hacked also increases. Users' information like username, password & post, etc. were shared if these values are published publicly then risk of it being affected also increases. In SSO account management is mainly done using central authentication site, i.e. no need of websites to authorize single user separately. In SSO authentication protocol mainly three characters play an important role.

User agent: user browser or end user which used to log into a website with the provided identifiers.

Relying Party: destination website where user wants to log in. A social website Zen desk etc.

ID provider: it allows only authenticate user to gain the services provided by the website or relying party, e.g. Facebook, gmail etc.

Here, for example using mondocam [7] as a relying party and twitter, Facebook and Google as an id provider's the user's credentials are stored in a single place so it becomes easy for an attacker to steal the data if information is provided in a weak website or in a malicious one.

978-1-4799-1753-2/15/$31.00 ©2015 IEEE

Fig 1:Facebook Twitter Login on Mondocam

is provided in a weak website or in a malicious one. There are mainly four scenarios which may occur The attacker may act as a client or end user who tries to confuse the relying party pretending to be the client and try to access the victims credential. An attacker may act as a relying party and make easier to believe that this is a trusted site and pretend to be the destination site to the victim [3].Victim unwarily passes the credential to the fake site. Attacker passes certain message which will be malicious one which causes user or victim to get trapped and able to gain the access.

II. LOGIC FLAWS PRESENT IN SSO SYSTEM

These whole problems lead us towards the logic flaws present mainly eight logic flaws were discovered which make us to concentrate more towards the development of the website. As more concentration is towards the logic flaws rather than about the social engineering. These logic flaws were found in both RPs & Idps code side and across login and account linking stages. As is known about this much vulnerability issues many new developments were made and protocols were also used to provide more security in SSO system, but unfortunately not all the problems were removed by using those protocols. Many logic flaws were discovered. Now elaborating this paper discusses what are the logic flaws discussed in the paper there are mainly eight logic flaws discussed in this paper.

RP developer's carelessness: developers are responsible for making a website strong or weak one. The developer should provide a secure wall which helps user credentials to be safe. Security problems.

Due to the API: implementing API is not an issue, but how to securely use API is more challenging. Before calling any of the API its pattern should be examined. Communication problem: the main problem is because of not having a proper communication any message. Integrated services in a single website: in a single website more than one service are integrating loading these much functionality.

Simplified web developing platform: now many technologies are available which simplified the usage of website development a beginner is now able to develop a website so they sometime they skip security steps and complicating it make the website more vulnerable.

The platform used for execution: some time developers of the API were not able to know about the functionalities of the browser, which makes it work so attackers will be attracted towards it. Weak authentication: authentication plays an important role in the SSO mechanism if an attacker is able to skip or bypass the authentication procedure, then SSO mechanism is of no use. So a strong authentication system is needed. User session does not expire: as user can access any functionality by just logging in once, then same method or functionality is provided when user wants to logout then he/she should be logout from all the respective accounts he was logged in.

Weak authorization: services should be provided to those who have their own profiles if they are not having authorized account, then they are not able to access any functionalities provided by SSO mechanism.

A.BRM analyzer :These logic flaws were discovered using an automatic tool, namely the BRM analyzer. This analyzer depends upon black box testing the analyzer parses across different sequential request, response messages it modifies http requests and responses. For decoding, deciphering or parsing we need a proxy here we are using Firefox's well known debugging tool firebug and fiddler are used. This analyzer mainly works in three stages:

I stage: Syntactic labelling stage: what all types of elements are there in messages these whole things are compared using lexical grammar.

II stage: Semantic labelling stage: after finding out the type of element need to find out the meaning of element used in the messages.

III stage: Adversary accessibility labelling stage: as both meaning and type of elements are found out next requirement to find out the error in the message.

III. STUDYING SSO SCHEMES ON MAJOR WEBSITES

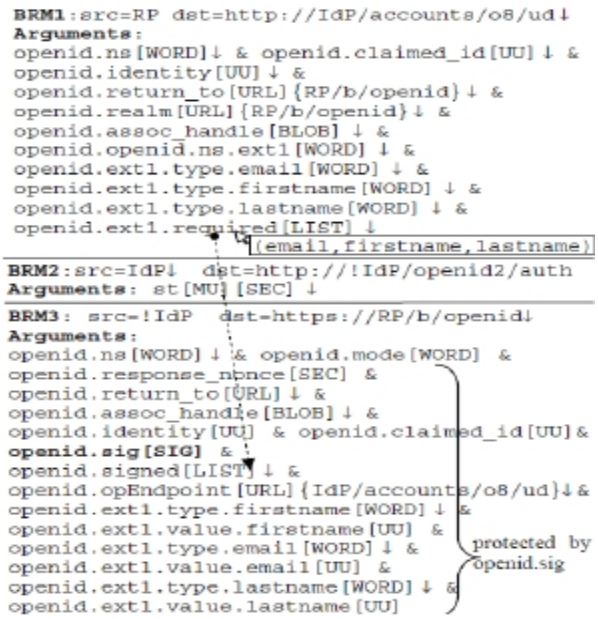
After completing these whole stages analyzers provides a dynamic output, which are mainly in HTML format makes a human developer or analyst to find out the problems and sort it out. Many IT companies were having these sort of problems which were discussed in the paper and using this analyzer they tried to figure out the problems and make the companies to know about these serious issues and they got acknowledgement from those companies regarding removal of that flaw or mistakes. Some of the companies are Facebook, Google, Jain Rain and PayPal etc.

A .Google Id:Google Id or Open Id [3] is an open standard for single sign on. This goggle id is based on open id. It uses to exchange information on top of the HTTP protocol. Anonymous ids or using multiple identifiers per user are some of the way used to make open it secure. Traditional password authentication is totally unsuitable for securing the access. The BRM analyzer is used to find out the meaning of traces and the flaws in the system.

Opened. ext1. Required in BRM1 is not provided with any security an attacker can easily access those data he can easily change the list provided as values are passed from this BRM1 then attacker easily skip the email id or any of the essential user credentials. As opened. ext1. Required is propagated to Openid. Signed

Opened. Signed in BRM3 this provides security to the data coming under this signature these data cannot be accessed without the concern of the user.

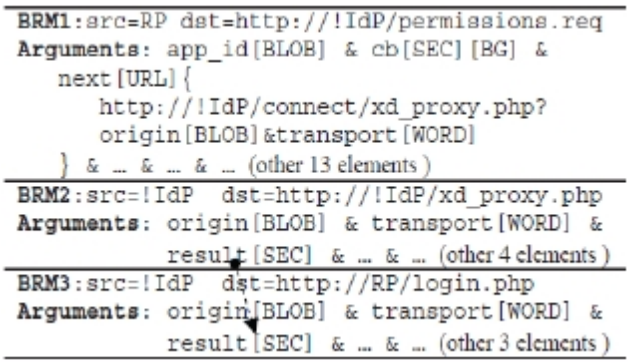
Opened. Signed in BRM3 as data here comes from the BRM1 then attacker can skip or remove the username or any of user's important credential which may create a serious logic flow



*B. **Facebook**:* Authentication on Facebook [6] helps the user to authenticate once and can access multiple functionality. A main flaw presents.

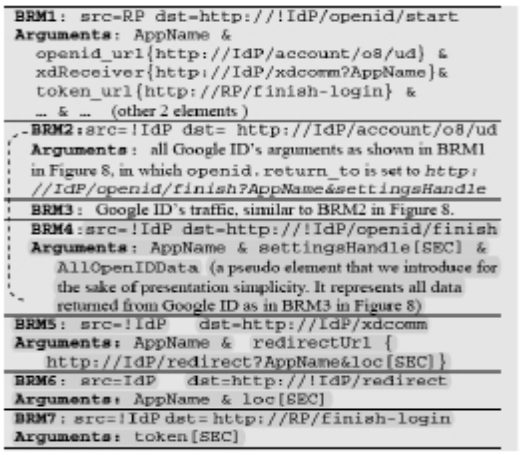
Here attack may succeed, if Facebook relies on the client-side same-origin-policy to pass the secret securely. Client-side mechanisms adobe flash. Let both Flash A and Flash B are loaded from Facebook (*fbcdn.net*). The secret is sent from Flash A to B (the same-domain communication). Flash B should be careful while sending the secret to an HTML

DOM in the intended domain (corresponding to the previous declared app_id).



C. JainRain

JainRain provides a way to social login and social sharing solution. The user registers themselves and provided with a unique identifier. It maintains a whitelist which access sites below white list.



JainRain checks against Whitelist twice, at first it checks the token. Bob can easily access the destination value & Gets settings handle Alice Visit bob's site Use handle w/ RP-APP in BRM2.

IV COMPARING WITH OTHER TOOLS

Many new tools and protocols were discovered by the protocol analysis community they are used to model and examine many security issues. Some of the techniques are a Millen's model, NRL analyzer & BAN logic.The NRL Protocol analyzer is a search tool which is given a particular goal and with the help of that goal

The user has to find out our search a path. SAML Single Sign [1] on main functionality is to exchange information securely across between online business partners. The SAML SSO protocol is mostly flexible because of the standard client mechanism and can be used on various platforms. An attacker can spoof DNS server using SAML 2.0. If any flaw related to authentication is present can be detected using LTL method. Liberty Enabled Client & Proxy Profile were 150 companies or more are now a days, providing their contributions and have a trust circle where a number of users exist who have a global network if any of the message is to be passed it is passed among these circles.

An attacker can access the information by injecting any malicious sites among this circle.We have many ways for getting the last message. In this paper we mainly focus towards the format of the http sequence of response's and requests.

V. CONCLUSION

Enterprises uses single-sign-on protocols mainly to reduce the cost and provide customer-care because of forgotten password and provide easy transaction and provide user with many user friendly features. Many political and judicial debates over Security of Web single-sign-on still exist .Using SSO mechanism is helpful as it helps to memorize only one password and can be able to access many accounts; it depends on particular sites trustworthiness. Companies should focus towards the authentication procedures. All flaws which were reported were fixed. Study shows quality of sso security deployments is not trustable.

REFERENCES

[1] Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuellar, Llanos Abad. "Formal Analysis of SAML 2.0 Web Browser Single Sign On: Breaking the SAML based Single Sign On for Google Apps," ACM FMSE, 2008.

[2] OpenID Wiki. "OpenID Phishing Brainstorm,"http://wiki. openid.net/w/page/12995216/OpenID_Phishing_Brainstorm

[3] Manuel Uruena and Christian Busquiel "Analysis of a Privacy Vulnerability in the OpenID Authentication Protocol," IEEE Multimedia Communications, Services and Security, 2010.

[4] S. M. Hansen, J. Skriver, and H. R. Nielson. "Using static analysis to validate the SAML single signon protocol," Workshop on Issues in the Theory of Security, 2005.

[5] Facebook. "OAuth Dialog," http://developers.facebook.com/docs/reference/dialogs/oauth.

[6] OASIS Standard. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, 2005.

[7] Pfitzmann, Birgit, and Michael Waidner. "Analysis of liberty single-sign-on with enabled clients." *Internet Computing, IEEE* 7, no. 6 (2003): 38-44.

[8] Nygren, Erik, Ramesh K. Sitaraman, and Jennifer Sun. "The akamai network: a platform for high-performance internet applications." *ACM SIGOPS Operating Systems Review* 44, no. 3 (2010): 2-19.

[9] Wang, Rui, Shuo Chen, and XiaoFeng Wang. "Signing me onto your accounts through facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services." In *Security and Privacy (SP), 2012 IEEE Symposium on*, pp. 365-379. IEEE, 2012.

[10] Meadows, Catherine. "Language generation and verification in the NRL protocol analyzer." In *Computer Security Foundations Workshop, 1996. Proceedings., 9th IEEE*, pp. 48-61. IEEE, 1996.

[11] Krishnamurthy, Balachander, and Craig E. Wills. "Privacy leakage in mobile online social networks." In *Proceedings of the 3rd conference on Online social networks*, pp. 4-4. USENIX Association, 2010

[12] Ellison, Gary, Jeff Hodges, and Susan Landau. "Security and Privacy Concerns of Internet Single Sign-On." *Liberty v1* 6 (2002).

[13] Wikipedia, "Secure Electronic Transaction," http://en.wikipedia.org/wiki/Secure_Electronic_Transaction