INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 2)
Available online at: www.ijariit.com

SSO Protocol Performance Testing

Rackymuthu
racky.rmuthu@gmail.com
Government Arts College, Coimbatore, Tamil Nadu

Buvaneswari
Buvann@gmail.com
Government Arts College, Coimbatore, Tamil Nadu

ABSTRACT

To build the SSO server, there is a need to identify better protocols among LDAP, SAML, and OIDC as these are protocols widely used. Best protocol can be identified based on testing at various levels. One way to test the protocol is based on its performance. So, LDAP, SAML, OIDC are tested based on their performance and OIDC is identified as the best performing protocol.

Keywords— *LDAP, OIDC, SAML, SSO*

1. INTRODUCTION

Single Sign-On is a secure and reliable network eco-system which keeps growing in complexity due to the interfaces with multiple user logging sub-systems for different applications and to ensure the safety of the network environment for everyone involved. Single Sign-On provides secure and reliable service in every system that has been specifically defined for overall security. Single Sign-On is shortly called SSO. SSO systems necessary requirements must be addressed. User identity management and different authentication mechanisms were defined together with the network protocols and standards to ensure a safe exchange of the information.

2. LITERATURE REVIEW

2.1 Research and Implementation of Single Sign-On Mechanism for ASP Pattern: Bo Li, Sheng Ge, Tian-yuWo, and Dian-Fu Ma

Software Services based Application Service Provider pattern is an important format to create the enterprise applications which integrates the business application with different authentication formats. So, there are queries such as repeated authentication and authorization format, complex authorization management, difficulty in describing security and information interoperability. Bo Li et al., stores resources in a uniform format, accesses it in a standard interface and exploits account federation, authentication, and authorization to transfer authentication and authorization results. As a result, Single Sign-On can be designed using this format.

Single Sign-On technology provides a convenient way to access systems in a distributed environment. The .Net Boarding pass uses Cookie and redirection to implement central authentication and distributed authorization. But it lacks the standard protocol to exchange authentication. But difficult architecture and authentication chain management are the shortcomings. So, it's hard to solve the Single Sign-On problem in ASP with traditional SSO technique.

Bo Li et al., tells, building on the SSO using SAML protocol is hard to implement. Surely SAML is a challenging protocol to build SSO, and also SAML has some disadvantages in security and architectural level. To resolve this challenge OIDC is the best option to build SSO.

2.2. Security Investigation, Analysis of OpenID: Alya I. Alqarni and Waleed A. Alrodhan.

OpenID is majorly used in identity management system (IdMS)y which identity providers (IdPs)and provide their users with open-identities that can be used to log in to particular relying parties (RPs). OpenID provides a single sign-on (SSO) solution that reduces the number of authentication credentials that are required. A Single Sign-On permits users to authenticate themselves to many SPs by using one set of authentication credentials. OpenID is easier and faster than the traditional method, which requires the user to manage a large number of digital identities since each SP only recognizes the identity it has issued.

Waleed A et al, provides an overview of OpenID and investigated its security. Also, conducted a security analysis of it. The analysis consisted of two parts; first, an analysis of the static of source code (written in C# language) using the VCG tool. This is finding four weaknesses in the code: unsafe code directive, code that appears to contain a hard-coded password, an application

that appears to log a user password, and .NET debugging enabled code. Secondly, an analysis of the HTTP messages uses OWASP ZAP tools.

Waleed et al., tells about the security investigation and OIDC authentication procedure. And Waleed et al., also explains about the phishing attack in the OIDC authentication procedure. Phishing attack means fraudulent attempt to obtain sensitive user information. But the communication between user input and OIDC is secured by JWT. Every communication between user and service is encrypted. So there is no possibility of phishing attacks.

2.3. Implications of Single Sign-On solutions on cloud applications: Mohamed Watfa, Shakir Khan, Ali Radmehr

The latest trend in businesses is moving towards one browser tool on portable hardware to access cloud applications which would increase portability but in the same situation would introduce security vulnerabilities. This resulted in the need for multiple layers of password authentication for cloud applications access. SSO is a tool that provides access control of multiple application systems. This research explores the effects and implications of Single Sign-On service on cloud applications. A latest framework of different information is developed by acquiring IT expert's opinions through extensive research to explore significant strategic parameters at the workplace. The framework was further tested using data collected from 400+ users in the UAE.

3. ALGORITHM VS PROTOCOL

A protocol is a set of rules that governs how a system operates. The rules establish the basic functioning of the different parts, how they interact with each other, and what conditions are necessary for a healthy implementation. a protocol doesn't tell the system how to produce a result. It doesn't have an objective other than a smooth execution. It doesn't produce an output.

An algorithm, on the other hand, is a set of instructions that produces an output or a result. It can be a simple script, or a complicated program. The order of the instructions is important, and the algorithm specifies what that order is. It tells the system what to do in order to achieve the desired result. It may not know what the result is beforehand, but it knows that it wants one.

- It's what needed to do to drive the car, the actions that the driver performs.
- The protocol is a set of rules that determines how the system functions.
- The algorithm tells the system what to do.
- The protocol means what is? The algorithm means what does?

LDAP, SAML, and OIDC are protocols. So choosing a better protocol from these protocols is very important. This selection needs a real time experimental operation. Here the performance testing is used to find the valid protocol. Calculating the login time of each protocol is the perfect way to identify the best SSO protocol. In this research LDAP, SAML and OIDC are the valid protocols considered for testing and the rest are outdated.

4. PROTOCOL COMPARISON

The system is implemented with three different mechanisms each for LDAP, SAML and OIDC. After the system implementation the user is allowed to login system with three different formats and their performance is assessed. Several login attempts of each format of protocols are collected.

Table 1: SSO Performance testing values in Milliseconds (ms)

Number of attempt	LDAP (Time in ms)	OIDC (Time in ms)	SAML (Time in ms)
1	45	160	180
2	52	161	172
3	130	125	160
4	39	139	182
5	43	55	205
6	41	110	192
7	50	119	187
8	71	130	178
9	43	132	169
10	48	120	194

While testing, every login attempt should be successful. If it is unsuccessful re-login and skip reading the measurement. The reason of login attempt failure may be due to network bandwidth problem or server unavailability or other technical issues. So, these are all common reasons for login failures.

The point of login time will start when the user clicks the button to login with the username and password. The point of login time will end at the point dashboard is opened. The in-between time of starting point and ending point is considered as a login time. In this in-between value lot of background and foreground jobs will happen to each protocol. This job's nature is different for each protocol. For testing 10 values related to ten different attempts are collected.

Table 1 contains the login time of the LDAP, SAML and OIDC protocols values in millisecond. These values represent the time that will take to login. Most of the time every attempt has a huge time difference compared to another protocol attempt. Login time of one protocol similar to another protocol is rare.

The standard deviation formula is used to find the best performance protocols.

$$\text{Standard Deviation} \quad s^2 = \frac{\sum(x_i - \bar{x})^2}{n-1}$$

Calculate the standard deviation of each protocol in the following steps.

1. Calculate the Mean of login values.
2. Subtract each login values from mean
3. Calculate the square root of each login value that is subtracted from mean values.
4. Add all the values for which square root is calculated.
5. Find the variance of the added values.
6. Find the standard deviation by adding the above values.

4.1 LDAP

Table 2: LDAP Performance calculation

x	$\bar{x}$	$(x_i - \bar{x})$	$(x_i - \bar{x})^2$
45	55	-10	100
52	55	-3	9
130	55	75	5625
39	55	-16	256
43	55	-12	144
41	55	-14	196
50	55	-5	25
71	55	16	256
43	55	-12	144
48	55	7	49
		Total	6801

Variance (S2) = 6801/9 => 755.6 and Standard deviation = 27.4

4.2 OIDC

Table 3: OIDC Performance Calculation

x	$\bar{x}$	$(x_i - \bar{x})$	$(x_i - \bar{x})^2$
160	125	35	1225
161	125	36	1296
125	125	0	0
139	125	14	196
55	125	-70	4900
110	125	-15	225
119	125	-6	36
130	125	5	25
132	125	7	49
120	125	-5	25
		Total	7977

Variance (S2) = 33947/9 => 886.3 and Standard deviation = 29.7

4.3. SAML

Table 4: SAML Performance Calculation

x	$\bar{x}$	$(x_i - \bar{x})$	$(x_i - \bar{x})^2$
180	125	55	3025
172	125	47	2209
160	125	35	1225
182	125	57	3249
205	125	80	6400
192	125	67	4489
187	125	62	3844
178	125	53	2809
169	125	44	1936
194	125	69	4761
		Total	33947

Variance (S2) = 33947/9 => 3771 and Standard deviation = 61

Table 2, 3, and 4 represent the performance calculations of the LDAP, OIDC and SAML protocols. The performance testing result tells 27.4 < 29.7 < 61 this mean LDAP < OIDC < SAML.

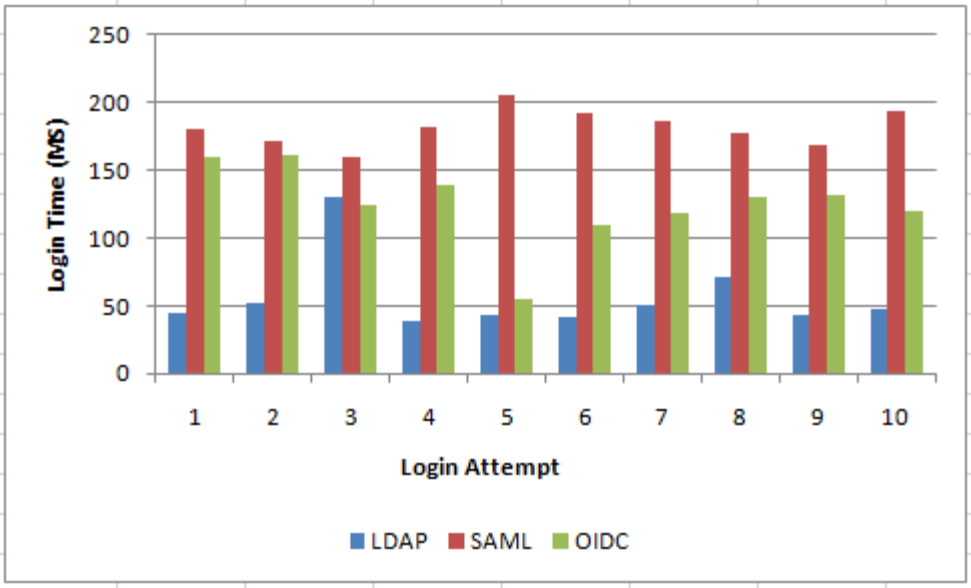

Fig. 1: SSO Protocol Performance Comparison

The above chart represents the different values related to each protocol. LDAP login time is the minimum because LDAP takes care of authentication. Due to this reason LDAP does quick login. The OIDC login time is higher than SAML. Moreover, this protocol takes care of the authentication. SSO focuses on authorization and SAML protocol takes care of authentication as well as authorization jobs. The reason behind this is the XML data format of SAML server is highly secure. This SAML secure data takes more time than the OIDC data for communicating with the client and server which is clearly depicted in figure 1.

Chart 2 displays the trend of each protocol. By using this different protocol can be compared. In LDAP and SAML values meet and cross only at one place. But the rest does not meet or cross. So, Figure 2 tells, each protocol login time has huge variation compared to other protocol. The bar and line chart represent the performance statistics of different protocols. The figure 2 pictorially represents that OIDC is better than the SAML.

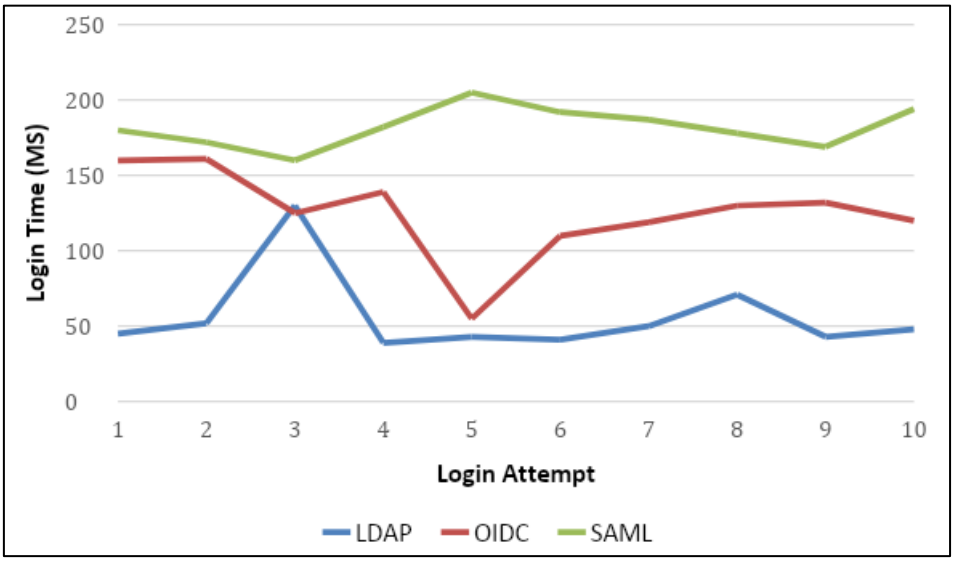

Fig. 2: SSO Protocol Trend comparison

5. CONCLUSION

The variation time between one attempt to another attempt is in milliseconds. It does not matter in a small-scale application with a minimum number of users using the application. But it matters when more users access the application. Here the standalone LDAP is not fulfilling the requirement for an SSO server. Even though SSO is only providing the authentication. LDAP protocol is considered for performance testing because the combination of LDAP and OIDC works as SSO Server. SSO servers can be built using OIDC alone. So, the real competition is between SAML and OIDC. Based on the test result, OIDC login time is better than SAML login time. This is averagely taken time that is not accurate. But this average time has an impact on the test result. The test result is concluded based on the average performance of these three protocols. These protocols produce different values. From the result it is concluded the protocol with the minimum time is used for login.

6. REFERENCES

[1] Arul Princy A., "A Survey on Single Sign-On Mechanism for Multiple Service Authentications" IJCSMC, vol 2, no. 12, pp. 40-44, Dec 2013.

[2] Armando A, Carbon R, Cuelar J, Compgna L, and Tobarra, L., "The Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-Based Single Sign-On for Google Apps" ACM New York, USA, pp. 1-10, Oct 2008.
[3] BaranTopal B., "Methods of Single Sign-On" KTH School of Information and Communication Technology, Dec 2016.
[4] Bo Li, Sheng Ge, Tian-yuWo, and Dian-fu Ma., "The Research and Implementation of Single Sign-On Mechanism for The ASP Pattern" Computer Institute, BeiHang, pp-12-18, Mar 2015.
[5] Busquiel C, Urueña M, "Analysis of a Privacy Vulnerability in the OpenID Authentication Protocol. Third IEEE International Conference on Multimedia Communications, Services, and Security "Multimedia Tools and Applications, Jan 2014.
[6] Bernardo Machado, Anderson C A, Nascimento, Rafael Tonicelli., "A Framework for Secure Single Sign-On" Springer Berlin / Heidelberg, Mar 2013.
[7] Caustn R P., "Smart Card Usage for The Authentication in Web Single Sign-On Systems" Helsinki The University of Technology, Dec 2002.
[8] Daniel Fett, RalfKüster, Guido Schmitz., "A Secure, Privacy-Respecting Single Sign-On System for the Web" ACM, Feb 2015.
[9] David R, Laurie R, and Chris M., "OpenID: The Definitive Guide" 1 edition ed. Oreilly Associates Inc, Oct 2012.
[10] Fang Ying lan, Jin Hao and Han Bing., "Single Sign-On Research and Expansion Based On CAS" The Open Cybernetics & Systemics Journal, pp 200-207, Jan 2014.

BIOGRAPHY

R. Rackymuthu
Student
Government Arts College, Coimbatore, Tamil Nadu

V. B. Buvaneswari
Assistant Professor
Government Arts College, Coimbatore, Tamil Nadu

