SECURING SINGLE SIGN-ON MECHANISM

[1]Yash Kedia [2]Amit Agrawal, [3]K. Chandrasekaran
Department of Computer Science& Engineering, NITK, Surathkal, Mangalore, India
Email:[1]yash.kedia2694@gmail.com, [2]amitagrawal1612@gmail.com, [3]kchnitk@ieee.org

Abstract- Nowadays the importance of authentication has increased for accessing your accounts registered for various applications on the internet. Due to increase in popularity of internet, people have started using internet for various purposes such as social networking, banking, e-commerce and many more activities in masses. The Single Sign-On (SSO) technology is increasing in demand as it is a benevolence for the users requiring multiple accounts. SSO has a schema with incorporated one-password based confirmation component at SSO server and local verification and approval at application's side. These activities require highly secure transmission due to involvement of confidential information. The main vulnerability point in this framework is authentication at the centralized server. This paper intends to propose a model which will reduce the vulnerability to maximum extent. This model merges the concepts of TPV (Third Party Verification), Diffie-Hellman key exchange and centralized authentication.

Keywords- SSO, Security and Third Party Verification

I. INTRODUCTION

A web service is a business application, which has a unique address on the Internet that can be accessed globally. World is shifting towards the use of internet for every need possible, so for these purposes one needs to authenticate himself on N number of web portals which can be stressful as remembering multiple strong passwords is not a piece of cake. Single sign-on (SSO) is a system whereby a solitary activity of client validation and approval can allow a client to get to all the web administrations where he has entry in all actuality as a user, without the necessity of giving his certifications once more.Thus Single Sign-On minimizes the effort of remembering multiple login credentials, a significant part of frameworks failure and is hence exceedingly alluring.

With the increase in number of users on web portals, the number of threats are also increasing which reduces the efficiency of the system and in some cases even results in loss of confidential data and wealth in case of financial transactions, thus increasing the vulnerability of SSO systems. So to secure the web services, we need to identify a mechanism which is least susceptible to attacks. Authentication is required to access the web services that are secure in which the user needs to provide identification. The primary concern after valid authentication is authorization. Authorization is used to establish connections between clients and web services providing them the permissions needed to perform various transactions.

SSO is the new development in this scenario to solve the work of multiple authentications and reducing the risk of attack on each web service authentication. This paper tends to give such a model which will provide secure transmission of user credentials at the centralized master level resulting in secure transmission of user's confidential data. This model will be able to detect threats such as man in the middle attack (MIM). This paper focuses on the secure establishment of connection between valid client and server and detecting any unauthorized attacker in the middle. After successful authentication, a service token will be generated for each session, which when terminated can't be accessed to access any information.

The paper is organized in the form of following sections. Section II consists of related work. Section III consists of proposed model. Section IV deals with attacks and system analysis. The subsequent sections consists of conclusion and references.

II. RELATED WORK

SSO is being developed and researched to provide ways of securing web services. Microsoft's Passport convention was the first endeavor at making a Web SSO framework, but it was never substantially put in use by non-Microsoft vendors. The adoption of this protocol was hindered as many security flaws were identified in it. Passport is by all account not the only Web SSO convention that had vulnerabilities. MDSSO alludes to the situation where SSO happens between security spaces worked by dissimilar associations. Rather than MDSSO electronic frameworks, some Web SSO frameworks give SSO inside a solitary association. They are called Web Initial Sign-On (WebISO) frameworks. WebISO frameworks normally give a web based part to an association's current single sign-on SSO schema, which in present state can't help online confirmation. Likewise remarkable is an alternate Internet2 venture called Shibboleth. Shibboleth handles both the online MDSSO and SSO inside an association, and implements SAML v1.1 [17].

SAML (Security Assertion Markup Language) is a standard that encourages the trade of security data. SAML is a XML-based system which empowers diverse associations (with distinctive security spaces) to safely trade validation and approval data. Numerous SSO administration suppliers like Google, Webex support SAML. The standard has risen as the go-to SSO convention for such applications. SAML got on rapidly with cloud-based suppliers, for example, Google, Webex and once conventional organizations, for example, IBM and Microsoft advocated SAML, it turned into the go-to SSO convention for some applications [16].

Kerberos based- Initial sign- on prompts the client to give username and password, which on check will deliver a ticket-granting ticket (TGT). Extra programming applications obliging validation, for example, email web administrations like yahoo mail utilize the ticket-granting ticket to claim their administration tickets, giving the client's credentials to the mailserver, without inciting the client to get re-authorized [4].

Smart card based- Firstly, it approaches the client for the smart card. Other web benefits likewise utilize this card, without hinting the client to re-enter details. It deals with the qualifications of the client put away on the smart card [4].

III. PROPOSED MODEL

The primary idea is to articulate a SSO model that provides credential management for all the web services on single server. The process of authentication in this model is built on password authentication scheme. This gives the benefits of simple usability in most web services that still use passwords for authentication.

Model Components
Following are the participants which make up our model:

1. Client (C): The web browser of the user acts as client on the behalf of user to access web services.

2. Centralized Authentication Server (AS): It is responsible for handling authentication and authorization services.

3. Web Service Provider (WS): It is the web service provider that requires client authentication before giving the client authorization.

4. Third Party (TP): It is responsible for generating random prime number P and random base G for securing the transmission.

The SSO model presented in this paper is the summation of the following steps:

1. The client requests for a web service (WS).

2. This service is redirected to an authentication service (AS).

3. AS requests client for username (UID) for validation of existence of such user in Database.

4. Client sends the UID for verification.

5. After successful verification, AS invokes Third Party (TP) and publically transports a dummy value of P and G.

6. TP sends P and G to AS and C.

7. C and AS generate random number and create the secret keys.

8. AS requests for password from C.

9. Then C sends H_1 -> password hashed with the secret key for validation.

10. After successful verification of H_1 with the local copy H_2 of AS, it authenticates C to WS and sends P and G to WS.

11. Then the connection is established between C and WS, and authorization privileges are provided to C accordingly by WS. The data is exchanged in encrypted form with the help of secret key.

IV. ANALYSIS OF THE SYSTEM

There are certain threats to user's confidential data that may occur while sending it over the network.

Man in the Middle Attack

The man in the middle attack (MIM) in machine security is a manifestation of dynamic listening in which the assailant makes autonomous associations with the exploited people and transfers messages between them, making them accept that they are talking specifically to one another over a private association, when truth be told the whole discussion is controlled by the aggressor [4].

MIM basically occurs during the process of establishing secure connection that is the key exchange process. As given in Diffie-Hellman's algorithm, when TP is not present, the numbers P and G is publically transported and the attacker may know it.

The secret key generated by the client and web service is as follows:

C-> $[(P)^a \bmod G] = L_1$ (Lets Say) AS-> $[(P)^b \bmod G] = L_2$ (Lets Say) Now

C-> $[(L_2)^a \bmod G] = X_1$ AS-> $[(L_1)^b \bmod G] = X_2$

Now $X_1 = X_2$ as we know by mathematical fundamentals: $X_1 = ((P)^a \bmod G)^b \bmod G = ((P)^a)^b \bmod G$
$X_2 = ((P)^b \bmod G)^a \bmod G = ((P)^b)^a \bmod G$ Thus $X_1 = X_2 = X$ acts as the secret key.

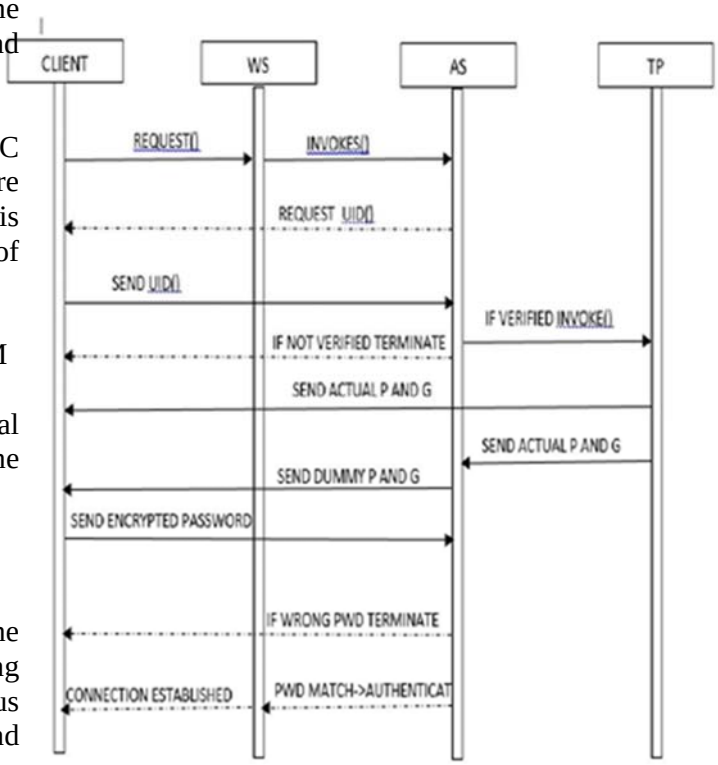

Fig. 1 Secure Connection Sequence Diagram

If P and G is known by the attacker, then value of a and b does not matter as attacker will choose a random number c and use it for generating two sets of secret keys one for client and another for authentication server, thus fooling the client and server in believing that the connection is secure.

As with the introduction of TP and the dummy values, the original G and P are not known by the attacker as TP send the value of G and P privately to C and AS.

Without knowing the actual values of G and P, the attacker cannot generate the right sets of keys. With the dummy values of G and P, attacker generates two sets of keys for C and AS respectively. These sets of keys are sent by him to C and AS which cannot be verified by them as they are wrong. This results in termination of connection which prevents the unsecure transmission of confidential data.

At present the most popular mechanism for securing SSO is SAML as it is faster and cheaper than other SSO mechanisms like OpenID and OAUTH2 which we have concluded after various researches on the Internet. It depends on "statements" about identities. It is expected that an AS is making a statement and that the AS is in charge of keeping up client credentials, confirming

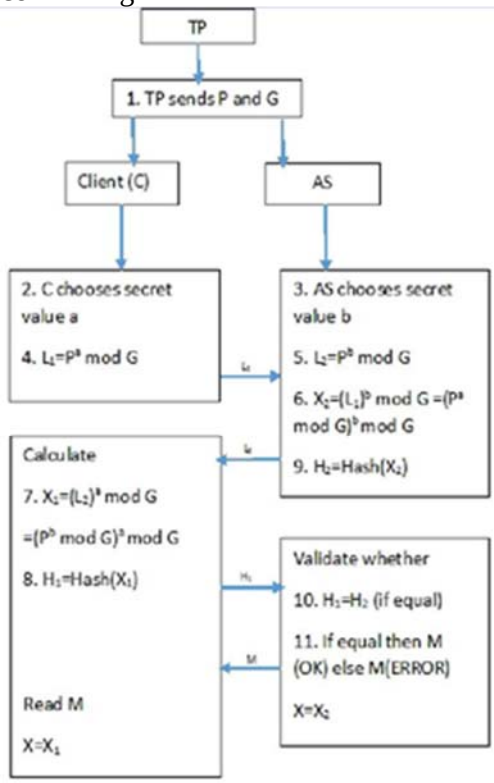

Fig. 2 Secure Key Exchange with the Help of Third Party

clients and deciding authorities. Our model uses TP(Third Party), that fools the attacker in believing that the TP does not exist [because of dummy values], thus reducing the chance of connection being compromised.Since our additive inclusion of dummy values leads the attacker to believe that he is hacking the correct link, it makes it very difficult for the attacker to try hacking our link with TP which send the actual values of p & g.

Our model aims to provide a secure transmission by adding this feature in pre-existing SAML model. Our model looks at the problem from the layman point of view, and tries to come up with a very simple and elegant solution for providing SSO security at minimal cost. Our models main focus is to remove MIM attack with minimal resources. This solution does not require any high order thinking, as it goes on a very basic way to solve the problems by fooling the attacker with dummy values without his knowledge.

V. CONCLUSION AND FUTURE WORK

In this paper we have proposed a Secure Single Sign on System to improve SAML with respect to the threat of Man in the Middle Attack. Our model uses the concept of Diffie-Hellman algorithm for secret key exchange with the additive inclusion of Third Party generation of P and G and transferring of dummy values of P and G between Client and Centralized Authentication Server for detection of Man in the Middle. The transmission of message takes place in encrypted form to maintain message layer integrity after securing the link by confirming the absence of MIM. Thus, our model provides a simple and cost-effective solution especially for smaller networks. In future, this model can be added with an efficient algorithm for selecting the TP server randomly to further minimize the possibility of attacker even knowing where to try to hack. Thus, it will provide an even more secure model which is already secured.

REFERENCES

[1] Yebin Chen, Bing Xia, Lianghong Shi and Baozhu Wu“Design of Web Service Single Sign On Based on Ticket and Assertion” Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011,pp297-300

[2] Web Single Sing-On Systems, [Online]. Available:http://www.cse.wustl.edu/~jain/cse 571-07/ftp/websso/

[3]Diffie-Hellman-Key-exchange, [Online]. Available:http://searchsecurity.techtarget.com /definition/Diffie-Hellman-key-exchange

[4] L.Wrage, S.Simanta, G.A.Lewis, and S.Jaspan, "T-check in Technologies for Interoperability: Web Services and Security-Single Sign-On", Software Research Institute Carnegie Mellon, 2007, pp 1-53

[5] Microsoft. net passport review guide

[6] J.Gantner, A.G.Schulz and A.Thede, "A Single Sign-On Protocol for Distributed Web Applications Based On Standard Internet Mechanisms", e-business and telecommunications networks Springer Netherland, 2006

[7] C.-C. Chang and C.-Y. Lee, "A secure single sign-on mechanism for distributed computer networks," IEEE Trans. Ind. Electron, Jan. 2012

[8] C.-L. Hsu and Y.-H. Chuang, "A Novel User Identification Scheme with Key Distribution Preserving User Anonymity for Distributed Computer Networks", Inf. Sci., 2009

[9] C.P. Schnorr, "Efficient Signature Generation by Smart Cards", J. Cryptology, 1991

[10] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," Wireless Commun., 2004

[11] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems,"Commun. ACM, 1978

[12] Single Sign-On, [Online], Available:http://www.replicon.com/customer-zone2/kb-2834

[13]Secure Authentication Blog for mobile SSO, [Online]. Available: https://www.secureauth.com/Resources/Blog.aspx?page=15

[14]Tivoli Software Information Center, [Online]. Available: http://www.publib.boulder.ibm.com