SINGLE SIGN ON CERTIFICATE BASED AUTHENTICATION FOR WS-SECURITY

Gaurav Sharma*
Gurleen kaur**

ABSTRACT

Web services, a set of heterogeneous different technologies diverse environment used in accessing resources of server is made secure using WS-security building block used conjunction with other web services providing requirements that describe method to encode binary security tokens to accommodate variety of authentication mechanisms. In this paper we are proposing Single sign on, a secure flexible architecture, a unified authentication mechanism for web services security needs by shifting the complexity of all integrated authentication mechanisms to so called SSO services serving as single point of authentication Single sign on is the most popular schema where user logs in once get accesses to all the systems to which server is connected via SSOA a plug-in installed at client side filtering out HTTP post and header and creating validating data with help of data returned by the authentication server. SAML and WS-security is used allowing authentication for cross sites by using SOAP method that encodes RMC into XML messages .Web services security issues have become more and more important .Web services based on the eXtensible Markup Language (XML), SOAP, and related open standards, and deployed in Service Oriented Architectures (SOA) allow data and applications to interact without human intervention through dynamic and ad hoc connections.. Certificate authentication implementing SSO is proposed making use of PKI infrastructure for Cross site encryptin session at both client and server side using SSL/TLS.

***KEYWORDS*:** SSO, SSOA, Authentication, certificate authority.

*Sr.Lect, JMIT Radaur Engg. College, YamunaNagar,India

** Lect, JMIT Radaur Engg. College,Yamuna Nagar,India

I. INTRODUCTION

A single sign-on assistant for web based applications, called SSOA, aiming at 'logging in once, running everywhere', with which we would solve uniform identity authentication among heterogeneous systems attaining simplicity, scalability and relatively low cost. This is an improved scheme to the centralized approach used for integrating different authenticating schemes for achieving unified authentication. Single sign-on (SSO) is a property of access control of multiple, related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them. As different applications and resources support different authentication mechanisms, single sign-on has to internally translate to and store different credentials compared to what is used for initial authentication. When name/value pair is received, a server deals with validation according to predefined processing logic. Hence, we can save HTTP POST data when a user logs in a system. When the user visits the page again, his/her request will be intercepted by the system, and then compose HTTP POST data after necessary processing. The data, afterwards, are sent to authorization components. As a result, user name and password inputting can be omitted. The login procedure can be executed by explorer monitoring program rather than the user. Web Services are arguably the most heterogeneous distributed technology ever Web services represents the next generation of distributed computing, building on and extending the current client-server model in some important ways. Web services adhere to a concept known as "loose coupling," which means services are discoverable, platform independent, and are expressed with self-describing interfaces. Companies have used application servers as central places to deploy their Web applications and business services. Such application servers become the access or integration points for all Web services. Application servers also play a major role in establishing trust context between the disparate Web services that need to integrate. Companies have used application servers as central places to deploy their Web applications and business services. Such application servers become the access or integration points for all Web services. Application servers also play a major role in establishing trust context between the disparate Web services

that need to integrate. .Security Challenges Specific to Web Services• Inter-enterprise Web services are dealing with untrusted clients. The Remote Procedure Call (RPC)-style services have special needs.

• End to end isn't just point to point:

• The creator of the message wrote the payload, but intermediaries may touch or rewrite the message afterwards.

Long-running choreographed conversations with multiple requests, responses, and forks.

• Clients and services do not have a way to negotiate their mutual constraints and capabilities before interacting.

• Securing Web services infrastructure needs XML's granularity:

• Encrypting or digitally signing select portions

• Standards for securing Web services are heavily PKI oriented.

• Trust management must be more robust for distributed computing to scale.

• Authorization policies are more difficult to write as environments become more loosely coupled.

• Intermediaries, particularly combined with attachments, make full protection more difficult. Web services providers must assure their customers that the integrity, confidentiality, and availability of information they collect, maintain, use, or transmit is protected.

The basic idea of the single sign-on security architecture is to shift the complexity of the security architecture to the so-called SSO service and thus release other parts of the system from certain security obligations. In the SSO architecture, all security algorithms are found in the single SSO server which acts as the single and only authentication point for a defined domain. Thus, there is a second benefit to an SSO approach to authentication/registration: a user has to sign-on only once, even though he may be interacting with many different secure elements within a given domain. The SSO server, which can itself be a Web service, acts as the wrapper around the existing security infrastructure that exports various security features like authentication and authorization. We will concentrate mainly on authentication in the SSO environment in this. The

SSO server enhances security of the whole system as the security credentials don't need to be passed around. The only point that accepts security credentials is the SSO server itself. Moreover, the SSO solution often allows federation, so the authentication can be performed in a broad scope (outside of the particular security domain) while the security credentials stay within the particular security domain.

II. RELATED WORK

Single sign on has been used in LDAP component matching technology for online certificate validation.SSO is used for federation access control model for each web service to get information about user whether trusted or not.SSO with trusted parties like Authentication providers some while get attacked by man in middle attacks now prevented by implementing it on trusted platform using hardware module. Various SSO solutions have been proposed that depend upon PKI, Kerberos, or password-store, but they require client side infrastructure and new administrative steps

Since HTTP is a "stateless" protocol, it is difficult to differentiate between visits to a web site, unless the server can somehow "mark" a visitor. This “marking” is done by sending a piece of state information (called a *cookie*) to the client. Any future HTTP requests made by the client to this server include this state. Many web applications have started to use cookies for session management and single-sign-on.

• Support multiple authentication systems such as name/passwords, certificates, one-time-passwords, etc.

• Support web access via middle tiers to legacy applications and provide name/password mapping

• Scale to hundreds of thousands of users

• Simple to administer and configure

• Support a whole range of deployment scenarios:

• Only one, to a few, physical web servers

• Only one logical web server (multiple physical) for

high availability and load balancing

• Many web servers (> 5) supporting many applications but within the same domain

• Multiple web servers spanning different domains

Wu kaing[**7**] proposes SAML based SSO unite authentication model extending Joint certifications spanning Different SSO domain using different authentications profiles but it still require to change united model, needs co-certifications and many changes are to be modified to prevent it from replay attacks.Andreas[**2**]proposes SSO system to be used by untrusted users based on trusted framework that uses an open scheme called IMPOSITOR that don't require to establish an external relationship between Service Providers and SSO authentication model but still it is difficult to be implemented in dynamically changing environment. In [**3**] David and Jim proposes CredX an open source to secure web and grid services facilitating secure storage of credentials and enable dynamic exchange of security tokens for different services but still it also faces many identity managements risks and failures and interoperations are difficult to maintain. In [**4**] Heong-kon-kim proposes component architecture model for WS-Security including different tiers for services area on basis of roles and their managements comprising integration of multiple services into single composite service and enhancing security measures through use of processes and packages but lacks interactive error checking and authentication mechanisms. Yang [**5**] proposes transmission model for security of SOAP messages used for communication between web services using XML signature and XML Encryption modes but still it lacks some more flags and secure attributes to avoid replay attacks. In [**8**] Wenjun Zhang addresses various ws-security threats and analyze integrated measures for web services to make them robust against attacks ensuring service-service authentication ,identity management ,trust relationship, different distributed authorization model & access management using role based, attribute based and risk adaptive access control but it did not show the exact way for integration just proposes the way to implement.

AUTHENTICATION MECHANISMS

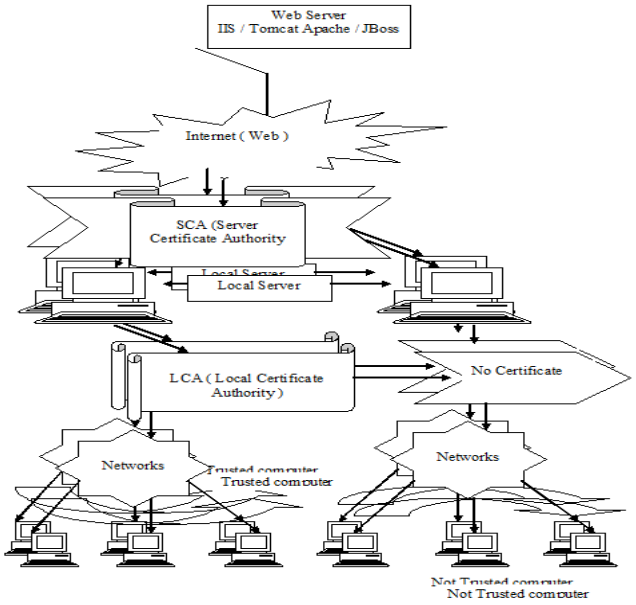
Many Authentication mechanisms were proposed earlier to authenticate hard core services to access web service, authenticating a consumer application with client certificate and propagating user ID of user authenticated. Now in this paper we are using SSO architecture implementing

certificate based authentication in a hierarchal order at local server, clients and at main server. Earlier certificate based authentication was implemented only in client side sessions someway does not meet the requirements of secure policies at both sides.

III. PROPOSED MEHODOLOGY

Using single sign on application, we can use certificate based authentications for different clients accessing web services. A certificate is a **"digital key"** installed on a computer. When the computer tries to access a server, the key will be automatically presented to authenticate the user. Client certificates can be mapped to Windows accounts in either a Domain or Active Directory. If we use the Windows Authentication Provider in ASP.NET, the application thread will run only for the user to whom the certificate is being mapped. For example, we can use the e-mail address (or a similarly unique field) contained within the certificate. And also from the client's perspective, security is seamless as the client is not required to log in using a logon page. This makes certificates an attractive option for automated business processes.

In order to run web services on SSL; you need to get certificate from the certificate authority like VeriSign; however in development environment sometimes you do not have certificate from valid Authority and need to generate self signed certificate. Microsoft provides a utility to generate self signed certificates.



Fig(i)Architecture of Certificate based hierarchal model

Certificate authority or certification authority (CA) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate. CAs are characteristic of many public key infrastructure (PKI) schemes. A CA issues digital certificates. that contain a public key and the identity of the owner. The matching private key is not similarly made available publicly, but kept secret by the end user who generated the key pair. The certificate is also a confirmation or validation by the CA that the public key contained in the certificate belongs to the person, organization, server or other entity noted in the certificate. A CA's obligation in such schemes is to verify an applicant's credentials, so that users and relying parties can trust the information in the CA's certificates. .PKI can be used to encrypt data communicated between two parties.

This can typically happen when a user logs on to any site that implements the HTTP Secure protocol. An SSL certificate provider (certificate authority) issues digital certificates to organizations or individuals after verifying their identity. These **SSL Certificate Reviews** can

help you choose one **SSL certificate provider** over another. Each SSL certificate provider has different products, prices, certificate features, and levels of customer satisfaction. In order to help you separate the wheat from the chaff, you can read authentic SSL reviews for each of the major certificate providers and decide who to trust with your SSL certificate needs. The above model is based on trust relationship, any trusted client at lower levels get access to resources at high levels that is also being a assigned identity for higher levels and more. So both the client and server side authentication is being implemented based on certificates issued and signed and authentication credentials passed automatically to higher authorities& user need not to sign again and again.

Certificate authority (CA) is a server in the domain that generates X.509 certificates that positively identifies entities and maintains a unique namespace of certificate owners. A certificate is considered to be tamperproof if signed electronically by CA .In this whenever client request to access resource of server a certificate not the public key is attached to the message and recipients verifies signature and then access public key thus preventing impersonation of keys. The certificate could be encrypted using XML encryption in transmitting mode. It is also in control of administrator to hide some of web services and allow access to the other different web services based on the credentials of trusted clients passed so ensures integrity of the web services being implemented in open source mechanisms.

IV.CONCLUSION

Securing Web services is complex and possibly overwhelming. Security must be incorporated into the planned requirements from the very beginning. Addressing a breach in security could be more expensive than implementing security measures in advance (cost of liability, public relations, loss of business, and so on). Also, security should be enforced throughout the infrastructure, both electronically and physically. Standards related to security are being developed by many standards organizations. Some of these standards are mature enough to be incorporated into your Web services applications today. Security for Web services is a necessity and can be deployed. Many of the methods have been deployed for security of web services like

WS-Trust, WS-Federation, WS-Security Policy, and WS-Secure Conversation. Web services providers must assure their customers that the integrity, confidentiality, and availability of information they collect, maintain, use, or transmit is protected. The confidentiality of information is threatened not only by the risk of improper access to stored information, but also by the risk of interception during transmission.

REFERENCES

[1] Fumiko Satoh, Takayuki Itoh, "Single Sign On Architecture with Dynamic Tokens," 2004 Symposium on Applications and the Internet (SAINT'04), 2004, pp.197.

[2]Impostor: A Single Sign-On System
for Use from Untrusted Devices., Andreas Pashalidis and Chris J. Mitchell, IEEE Communications Society,2004.

[3] Cheng Yang, Jianbo Liu, Jiayin Tian, Yichun Zhang," Authentication Scheme and Simplified CAS in Mobile Multimedia Broadcast," icmecg, 2009 International Conference on Management of e-Commerce and e-Government, 2009, pp.517-521.

[4] J.S. Park, R. Sandhu, "Binding identities and attributes using Digitally signed certificates," acsac, 16th Annual Computer
Security Applications Conference (ACSAC'00), 2000, pp.120.148

[5] Eun-Ju Park*,Haeng-Kon Kim* "Web Service Security model Using CBD Architecture" 2007, 0-7695-2867-8.

[6] Jeremy Goold, Mark Clement, "Improving Routing Security Usinga Decentralized Public Key Distribution Algorithm," icimp,Second International Conference on Internet Monitoring and Protection (ICIMP 2007), 2007, pp.8.

[6] Fei Zhu, Qiang Lv, "ACEAC: A Novel Access Control Model for Cooperative Editing with Workflow," isecs, 2008 International Symposium on Electronic Commerce and Security, 2008, pp.1010-1014.

[7] Enrique de la Hoz, Antonio Garcia, Iván Marsá-Maestre, Miguel Ángel López-Carmona, Bernardo Alarcos, "An Info card-Based Proposal for Unified Single Sign on," saint, 2009 Ninth Annual International Symposium on Applications and the Internet, 2009, pp.231-234.

[8] Wenjun Zhang"Integrated Security Framework for Secure Web Services" 978-0-7695-4020-7, 2010 IEEE.

[8] Fumiko Satoh, Takayuki Itoh, "Single Sign On Architecture with Dynamic Tokens," saint, 2004 Symposium on Applications and the Internet (SAINT'04), 2004, pp.197.

[9] Wei Huang, Jinhua Xu, "M4WebGIS: A Mobile Agent-Based Middleware for WebGIS", wcse, Second International Workshop on Computer Science and Engineering, 2009, pp.234-238.

[10] Fang Ying-lan, Han Bing, Li Ye-bai, "Research and Implementation of Key Technology Based on Internet Encryption and Authentication," 2009 International Conference on Networking and Digital Society, 2009, vol. 1, pp.179-182.