Research on Security Model of Web Service

Jia-ju WU*, Xing-lin ZHU, Zheng-ji LIU and Zheng CHENG

China Academy of Engineering Physics, Institute of Computer Application. Mianyang Sichuan, 621999 P.R. China

*Corresponding author

Keywords: Web service, Security, Model.

Abstract. With the widely using of Web Service, its security is more and more important. For these requirements, series specifications are put forward by W3C. Based on studying these criterions, a web service security disposal method is provided in this paper, which uses security mechanism of transport layer and application layer. This method constructs point to point and port to port configuration web service security model which is based on WS-Security, WS-Policy, WS-Trust, WS-Privacy, WS-Secure Conversation, WS-Federation, WS-Authorization...etc. At last this model is integrated with application system security model and used to realize access control.

Introduction

The key ability of Web service [1] is to provide a comprehensive, comprehensive, interactive, and easy to integrate solution. Web services in providing solutions to solve the problem of the same time, the security problem is far greater than the traditional program. Web service in a single transmission solution or ordinary firewall is unable to ensure the security of Web services. They lack the following features: end-to-end protection, non-repudiation, selective protection (part of protection message), authentication mechanism and flexible message protection. Therefore, based on the study of Web security service specification (including WS-Security, WS-Policy, WS-Trust, WS-Privacy, WS-Secure Conversation, WS-Federation, WS-Authorization) is proposed based on the mechanism of safety of transport layer and application layer to solve the problem of Web service security.

Term Definition

Because the terms are different in various technologies, this document defines a number of terms that can be consistently applied across different security formats and mechanisms. As a result, the terms used here may be different from other specifications, which are defined in order to enable readers to map them to their preferred vocabulary.

Web service: describes the application components, application functions and interfaces of these components are SOAP, including through XML, WSDL and HTTP, the existing and emerging Web technology standard is open to potential users. Compared with the Web site, the browser based interactive platform or related technology, Web service is a platform and language independent manner, by defining the format and protocol, from computer to computer services.

Token Security: to express security related information (for example, X.509 certificate, Kerberos notes and authentication, mobile devices from SIM card security token, user name, etc.).

Security Token Signed: signed security token as a security token, it contains a set of relevant statements signed by the issuer with a password (assertion). Examples of signed security tokens include X.509 certificates and Kerberos notes.

Claim: a statement is either a statement on the subject, or a statement made by the subject or the dependent party associated with the statement.

Subject: the theme of security token is a subject (for example a person, an application or a business entity), the expression of the security token is applied to the main body. Specifically, the subject is the owner of a security token that has the information needed to prove the ownership of the security token.
Proof-of-Possession: the information that is used in the process of proving a security token or a group of claims. For example, the ownership certificate can be a private key that is associated with a security token that contains a public key.

Web Service Endpoint Policy: Web service in the specified processing message required to declare. Endpoint strategy can be expressed in XML, and can be used for authentication and pointed out (for example user or group ID certificate.), authorization (e.g. certain executive ability proof.) related requirements or other custom needs.

Claim Requirement: a declaration of the need to be able to rely on the whole message or some elements of the message, all the operations of a given type or only in a certain environment, some operation. For example, when the number of requests to purchase exceeds the specified limit, the service may require the applicant to prove his or her rights.

Intermediary: when a SOAP message is sent from an initial request to a service, some of the media that performs the routing message, or even changes the message, may operate on the message.

Actor: a participant is an intermediary or endpoint (such as defined in the SOAP specification), it is identified by the URI, and processing SOAP messages. User or client software (e.g., browser) is not a participant.

Web Service Security Model

Web services can be accessed by sending an SOAP message, requesting a specific operation, and receiving a SOAP message response (including an error message) by sending a URI message to the service endpoint identifier. So Web service security contains tools to protect the integrity and confidentiality of messages, as well as the tools used to ensure that services are acting only on requests that are declared in the declaration policy. At present, the secure sockets layer (SSL) and the actual transport layer security (Layer Security Transport, TLS) are used to provide transport level security for web services applications. SSL/TLS provides several security features, including authentication, data integrity, and data confidentiality. SSL/TLS enabled point to point security session. IPSec is another network layer standard for transport security, and it may become important for Web services. Like IPSec, SSL/TLS also provides a secure session with host authentication, data integrity, and data confidentiality.

The current Web service applications to mobile devices, gateway topology, agent, load balancer, "demilitarized zone" (demilitarized zone, DMZ), data center outsourcing (outsourced data center) and the combination of many things system dynamic configuration of global distribution, together. All of these systems are dependent on the ability of message processing intermediaries to forward messages. In particular, the SOAP message model operates on the logical endpoints of abstract physical network and application infrastructure, so it is often integrated with the middle of a multi hop (multi-hop) topology.

![Figure 1. Web service security model of point to point configuration.](image1)

![Figure 2. Web service security model for end to end configuration.](image2)
message content. Point to point configuration of the web security model is shown in Figure 1, end to end configuration of the web security model is shown in figure 2.

Point to point configuration and end to end configuration of the Web service security model can achieve the purpose of security control through the following process:

Web service can request a message to prove a set of declarations (for example name, key, license, performance… etc.). If the message arrives but does not have the required declaration, the service may ignore or reject the message. We call this set of necessary statements and related information called strategies.

A request may be associated with a message that the security token is associated with a message that is required to be declared. In this way, the message is not only required for a particular operation but also to prove that the sender has a claim for the operation.

If a request is not required, the requesting person or their representative may obtain the necessary statement by contact with other Web services. These other Web services, which we call security token service (token security service), can be followed by a set of statements that require them. Token Security service agents trust between different trusts domains through the issue of security token.

Security token service model as shown in Figure 3, any request can also be a service, security token service can also be a Web service, and including the expression of the policy and security token.

Declarations, policies, and security token security models contain and support several more specific models, such as identity based security, access control lists, and performance based security. It allows the use of existing technologies such as X.509 public key certificates, Kerberos shared secret notes, and even password summary. It also provides an integrated abstraction that allows the system to build a bridge between different security technologies. The model is sufficient to establish a more advanced key exchange, authentication, authorization, and auditing trust mechanism.

**Web Services Security Specification**

The Web service security model is supported by the Web service security standard. The hierarchical structure of the Web service security specification is shown in the following figure:
WS-Security: how to describe the additional SOAP message signature and encryption header. In addition, it also describes how to add security tokens to messages (including binary security tokens, such as X.509 certificates and Kerberos notes).

WS-Policy: the ability and constraints to describe the security (and other business) policies of the intermediary and endpoints (e.g. the security token required, the encryption algorithm and the privacy rules that are supported).

WS-Trust: a framework that describes the trust model that enables Web services to be interoperable securely.

WS-Privacy: a model that describes how Web services and requests are declared subject to privacy preferences and the organization's privacy practices.

WS-Secure Conversation: will describe how to manage and authenticated message exchange among all parties, including the security context switch and the establishment and derivation of the session key.

WS-Federation: will describe how to manage the trust relationship in the environment of heterogeneous coalition, including support for federated identity.

WS-Authorization: describes how to manage authorization data and authorization policies.

Web Service Security Model and the Current Security Model Integration

Web service security model is compatible with existing security models that are commonly used for authentication, data integrity, and confidentiality of data. It is possible to integrate the solution based on Web services with other existing security models.

1) Security Transport: existing technologies, such as secure sockets (SSL/TLS), can provide a simple point to point for the integrity and confidentiality of the point. Web services security model to support the existing security transmission mechanism and WS-Security (and other specifications) are used together to provide (especially across multiple transmitters, intermediary and transmission protocol) end-to-end confidentiality and integrity.

2) PKI: advanced PKI model relates to a certificate authority that issues a certificate with a public key, and a body that is in harmony with an organization (e.g., a property institution) that is in addition to the ownership of the key. The owner of this certificate can use the associated key to express multiple declarations (including identity). Web service security model supports security token service using public asymmetric key issue security token. The meaning of PKI is the most widely used, and it does not use any special level or model.

3) Kerberos: Kerberos model with the key distribution center (KDC) communication, using symmetric key encryption key for this issue, both sides are locked, and they will be “introduced” to each other, to the trust between the parties. Once again, the Web service model based on the core model, and the security token service through a security token issued with the symmetric key encryption and encryption to entrust agent trust.
Application

The typical application of web service security model is access control. Web service security model in the access control of the application of the case is analyzed below. For example, when working together, Alice and Bob find that they often have to negotiate with each other and establish a trust level. As a result, Alice wants to allow Bob to schedule meetings without having to delegate it every time. She can increase the duration of the delegate security token, but need to reissue the token, if she wants to repeal the ability to schedule the meeting schedule Bob, it will be more trouble. Bob and web through the Alice service access control process as shown below:

Alice with her schedule service communications (certified her own) get authorization list. She updated the authorization list to allow Bob to view her idle or business data, schedule meetings and submit data to the service. Now, when Bob visits her schedule for these operations, he does not need a security token from Alice.

Conclusion

Existing Web service architecture is lack of effective security support, web service security is the industry's most concerned about the problem. Based on the research of web security specification on the Web service security model using the transport layer and application layer mechanism is proposed, the solution can solve the point to end protection, non-repudiation, selective protection of the point and the end (a part of the problem, protect the message) flexible authentication mechanism and message protection etc. Many of the criterions are still in development. So open, universal, complete Web service security standards still need to be further studied.

References