PROTECTION OF WEB SERVICES

Norqobilov Hakimbek Nuriddin o'g'li
Temiz State University graduate student

https://doi.org/10.5281/zenodo.7990090

Due to its nature (loosely bound connections) and use of open access (mainly HTTP), SOA implemented by web services adds a new set of requirements to the security landscape. The security of web services includes several aspects:

Authentication is verifying that a user is who they claim to be. A user's identity is verified based on the credentials provided by that user, such as: Something has credentials issued by a trusted authority, such as a passport (real world) or a smart card (IT world). Someone knows, for example, a shared secret, such as a password. One thing, for example, biometric information.

Using a combination of several types of credentials is called "strong" authentication, for example, using an ATM card with a PIN or password (something someone knows) (there's something).

Authorization (or access control) - granting access to certain resources based on the rights of the authenticated user. Rights are defined by one or more attributes. An attribute is a feature or characteristic of a user, for example the attribute "conference speaker" if "Marc" is the user.

Privacy, secrecy - keeping information secret. A message, such as a web service request or e-mail message, also includes the identity of the sender and receiver in a confidential manner. Privacy and confidentiality can be achieved by encrypting the message content and obfuscating the identities of the sending and receiving parties.

Integrity, Non-repudiation - Ensuring that the message has not been altered during transmission by digitally signing the message to the sender. A digital signature is used to verify the signature and ensure non-repudiation. After the timestamp in the signature expires, no one will be allowed to read the message again.

The security requirements of web services also include credential mediation (the exchange of security tokens in a trusted environment) and service capabilities and limitations (determining what a web service can do under what circumstances).

In many cases, Web services security tools such as Oracle WSM rely on public key infrastructure (PKI) environments. PKI uses cryptographic keys (mathematical functions used to encrypt or decrypt data). Keys can be private or public. In an asymmetric encryption model, the receiving party's public key is used to encrypt the plaintext, and the receiving party's corresponding private key is used to decrypt the ciphertext. Also, the private key is used to create a digital signature by signing the message, and the public key is used to verify the signature. Public key certificates (or certificates for short) are used to guarantee the integrity of public keys.

Transport level security. Secure Socket Layer (SSL), otherwise known as Transport Layer Security (TLS), is the Internet Engineering Task Force's (IETF) officially standardized version of SSL, the most widely used transport layer data transfer protocol:

Authentication (communication is established between two trusted parties).

Confidentiality (exchanged data is encrypted).

Message integrity (data is checked for possible corruption).

Secure key exchange between client and server.

SSL provides a secure communication channel, but when the data is not "in transit", the data is not protected. This makes the environment vulnerable to attacks in multistage transactions. (SSL provides end-to-end security as opposed to end-to-end security.)

Application-level security complements transport-level security. Application-level security is based on XML frameworks that define confidentiality, integrity, and authenticity; message structure; trust management and federation.

Data confidentiality is ensured by XML Encryption. XML encryption specifies how digital content is encrypted and decrypted, how the encryption key information is transmitted to the recipient, and how the encrypted data is identified to facilitate decryption.

Data integrity and authenticity is ensured by XML Signature. An XML signature associates the identity of the sender (or "signer") with the XML document. Signature and signature verification can be done using asymmetric or symmetric keys.

A signature ensures that the signer is not repudiated and verifies that messages have not been modified since they were signed. Message structure and message security are implemented by SOAP and its security extension WS-Security. WS-Security specifies how to attach XML Signature and XML Encryption headers to SOAP messages. In addition, WS-Security provides profiles for 5 security tokens: Username (with password digest), X.509 certificate, Kerberos ticket, Security Assertion Language (SAML) assertion, and REL (rights assignment) document.

The body of a SOAP envelope contains the business payload, such as a purchase order, financial document, or simply a call to another web service. SAML is one of the most interesting security tokens because it supports authentication and authorization. SAML is an open framework for exchanging security information over the Internet via XML documents. SAML consists of 3 parts:

SAML Assertion - How you define authentication and authorization information.

The SAML protocol is how you ask (SAML Request) and receive the necessary confirmations (SAML Response).

SAML Bindings and Profiles — How SAML assertions work "on" (Bindings) and "in" (Profiles) industry-standard transport and messaging systems.

The full SAML specification is used in browser-based federation cases. However, Web services security systems such as Oracle WSM use only SAML assertions. The protocol and connections are controlled by WS-Security and a transport protocol such as HTTP.

References to SAML assertions and assertion identifiers are contained in the WS-Security Header element, which in turn is included in the SOAP envelope header element (described in the WS-Security SAML token profile). The SAML security token is especially relevant in situations where identity distribution is important

References:

1.Galatenko V.A. Fundamentals of information security. "University of Information Technologies"

2.Alimov R, Khodiev B, Alimov Q and others. "Information systems and technologies in the national economy", T: "Sharq"-2004.

3.Alimov Q, Abduvahidov A and others. "Fundamentals of information technology" Study guide. T: - TDIU, 2003.

4.https://docs.oracle.com