International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

E-ISSN: 2321-9637

Securing Web Services Based on XML Signature and XML Encryption

Sonali G. Gadwar[1], Asst. Prof. Dhananjay Sable[2]
Department of Computer Science & Engineering [1, 2]
Email: sonaligadwar@yahoo.co.in

Abstract- XML is spreading quickly as a format for electronic documents and messages. As a consequence, greater importance is being placed on the XML security technology. With the development of web services application, some issues of web services security are increasingly prominent. As a platform-independent language, XML is widely used for its high expansibility. T his paper formulates the XML signature and encryption as the core of web services security technology, and describes how to create and verify XML signature, how to encrypt and decrypt XML data. The application of XML signature and encryption in the Web services security is illustrated.

Index Terms- Web services, XML signature, XML encryption, XML Security**.**

1. INTRODUCTION

When more and more products integrate Web services characteristic into their concentrate, Web services can be applied to the solution of the application program extensively. The problem of Web services security is outstanding day by day. Web services use the messages method based on XML to create and access services, thus, XML security is the security foundation of Web services. In order to guarantee the security in using XML as the media of information exchange effectively, especially the sensitive information described in XML, it can be deal with by combining with XML signature and encryption.

2. TRADITIOANL SECURITY TECHNOLOGY

From table 1 we can find that all of the web services messages transmit through the application layer. Thus, the security may be guaranteed by the safety mechanism of present network level.

Table 1. Protocol stack of web services

UDDI	Service Discovery and Publication
WSDL	Service Description
SOAP	XML-Based Messaging
XML	eXtensible Markup Language
HTTP FTP SMTP	Network

Although SOAP and HTTP (or SMTP, FTP and so on) has been enough for interoperability XML messages transmission, and WSDL also could fully transmit what messages service between requester and provider needs, but complete demand of covering the electronic commerce and so on must also need more security considerations. At present already had a set of readymade transmission level safety mechanism SSL (HTTPS) which moreover widely accepts, but only depends upon SSL can not to be able to in situation of providing enough secure in the Web service model:

- The SSL safety mechanism is not necessarily suitable for other transmission mode which will realize in the future of the Web service, for example, SMTP, TCP, FTP, messages formation, and so on.
- SSL only can carry on the encryption to the complete information, but cannot have the choice to carry on the encryption to the partial information, when transmission mass data like this, will cause the serious performance question.
- SSL can only guarantee point-to-point security, but is unable guarantee safeguards the end-to-end security. Although SSL may guarantee that the SOAP news between the node is safe, but because news is by the definite orders way existence in the node interior SOAP, therefore once the node is taken over control by the aggressor, he may examine that even tampers with the SOAP news. Therefore, regarding the Web service, the end-to-end security is very important.

In summary, the current safety transmission mechanism cannot adapt the request of Web services security, needs to formulate the new security specifications. In logic package of safe service, those who enhance the usability more is to take consideration from the physical level and the network level, therefore the new security specifications more concentrate in the confidentiality, integrity, undeniable, distinction and authorized aspect. The XML form's security (by the XML form expressed

that data security) was one kind of developed profession standard .XML signature and encryption in itself is not an item of safety work of Web services, but XML signature and encryption is the foundation component of many safety work of Web service. This technology joined some elements in the XML documents to use for sealing and enciphered data and the encryption method, etc, which has realized the confidentiality, the distinction, the integrity, undeniable of XML document, and so on[1].

3. WEB SERVICES SECURITY

Web Services, like common web applications, relies on the same HTTP transport protocol and the basic web architecture. Hence it is susceptible to similar threats and vulnerabilities. Web Service Security (WS-Security) is a flexible and feature-rich extension to SOAP to apply security to web services [3].

Some of the basic concepts that Web Services Security are based upon are:

1. Identification and Authentication: Verifying the identity of the user, process or device to allow access to a resource or information system.
2. Authorization: The permission to use a resource
3. Integrity: The property that the data has not been modified in any unauthorized manner while in storage, processing or transit.
4. Non-repudiation: Non-denial by either sender or receiver of having sent or received the information, respectively.
5. Confidentiality: Preserving authorized restriction and information access.
6. Privacy: Restricting access to subscriber or relying party information in accordance with Federal Law and organizational policy.

3.1 *Ws-security architecture*

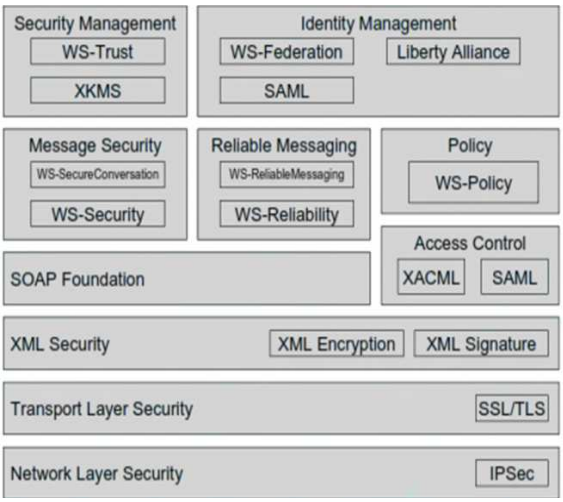

Fig. 1 WS-Security Architecture

The open community that created Web Services developed a number of security standards for Web Services. The above reference model maps these standards to the various layers of the standard Web Service [3].

- WS-Trust: Describes a framework for trust models that enables Web Services to operate securely.
- WS-Policy: Describes the capabilities and constraints of the security policies on intermediaries and endpoints.
- WS-Privacy: Describes a model for how Web Services and requesters state privacy preferences and organizational privacy practice statements.
- WS-Security: Describes how to attach signatures and encryption headers to SOAP messages.
- WS-Federation: Describe how to manage and broker the trust relationships in a heterogeneous federated environment including support for federated identities.
- WS-Secure Conversation: Describe how to manage and authenticate message exchanges between parties including security context exchange and establishing and deriving session keys

4. XML SIGNATURE

Carrying on the signature to the XML document's specific part is a very essential function. If only can carry on the overall signature to documents, the revision again to the documents will be unable to make when finishing sign.

4.1 *Overview*

XML Signature is an electronic signature technology that is optimized for XML data. The practical benefits of this technology include Partial Signature, which allows an electronic signature to be written on specific tags contained in XML data, and Multiple Signature, which enables multiple electronic signatures to be written. The use of XML Signature can solve security problems, including falsification, spoofing, and repudiation.

4.2 *Comparing with the traditional digital signature*

Compares with the traditional digital signature, What XML digital signature returns is XML form signature result with the <Signature>element expression, But what tradition digital signature returns is a string primitive or the binary data undergoes the code.

1) XML signatures are suitable for the network environment of distribution

Traditional digital signature technology sent the signature value and the original message to the Verify Caller for Authentication, not only has increased current capacity of the network, aggravated the bilateral burden, also has affected the efficiency of signature confirmation. The XML digital signature has profited from URI modeling thought of Internet the resources, the data waiting to sign use the URI modeling, the data quotation and processing conforms to the characteristic of distribution network.

2) Type of sealing

The result of XML digital signature's returns to a XML element, it uses the <Signature> element and daughter element to present the signature value as well as all confirmation information. According to needs to release, putting <Signature> element in any position of documents, but will not destroy the structure of XML documents. The position is relation of signature element and signed data in identical XML documents.

3) Expression form of signature key

The traditional digital signature uses X.509 certificate to express the type and value of signature key. XML digital signature as far as possible hardly relies on the special-purpose form of processing signature, to enhance the XML the probability of signature result, use the element <Key Value> and its daughter element to express all information of signature key clearly and simply.

4) The lamination confirmation model of XML signature

When tradition digital signature carries on verifying and signature, it will only return two kind of possible results: Signature is effective or invalid. The confirmation signature of XML digital signature uses the lamination confirmation model, carries on the confirmation separately to different part of digital signature; the application procedure makes the trust decision-making according to the confirmation result of different level to meet the actual needs.

4.3 Xml signature structure

Table 2 and fig.2 shows an example of an XML signature format and XML data that is XML-signed. An XML signature is a document structure with the <Signature> element at its top. Under the <Signature> element, lies its child elements, including a <SignedInfo> element, which contains references to the algorithm used for the XML signature creation and to the target XML data. It also holds digest value and other information, a <SignatureValue> element that contains the signature value, and a <KeyInfo> element that contains the public key certificate information to be used when the XML signature is verified. When considering the characteristics of XML Signature, the <Reference> element, which is a child element of the <SignedInfo> element is particularly important. Multiple <Reference> elements may be contained in the <SignedInfo> element. This enables any number of XML data segments at any location to be signed. This feature ensures that an extremely flexible system can be built up by using XML Signature. Among them, '?' express 0 or 1 match, '*' express 0 or a lot of match, '+' express 1 or a lot of match [1, 2].

Table 2. Xml signature format

```
<Signature ID ?>
  <SignedInfo>
<CanonicalizationMethod/>
  <SignatureMethod/>
  (<Reference URI ?>
  (<Transforms/>) ?
  <DigestMethod>
  <DigestValue/>
  </DigestMethod>
  </Reference >) +
  </SignedInfo>
  <SignatureValue/>
  (<KeyInfo/>) ?
  (<Object ID ? />) *
  </Signature
```

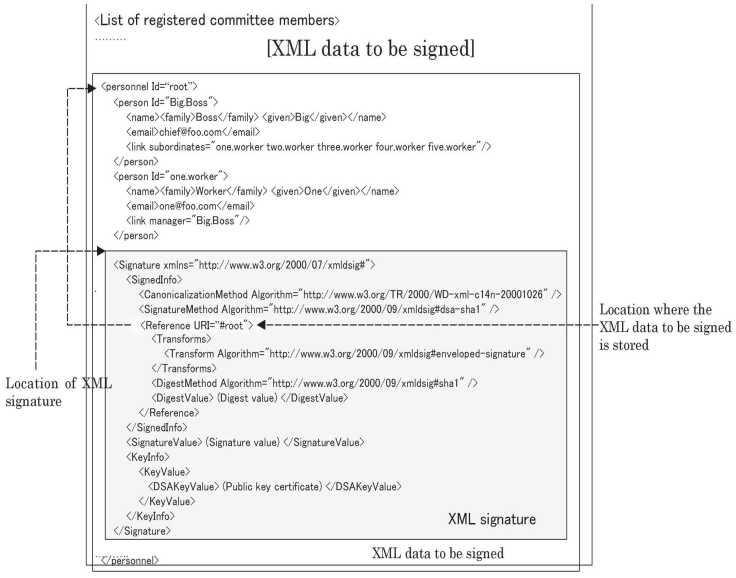

Fig. 2 XML signature format example.

4.4 Formulation and verification xml signature

1) Formulation of XML signature

Formulation the XML digital signature includes the following several steps:

a) Determine the URI that to be signed;

b) Calculate the value of summary;

c) Pack the summary into the <Reference> element; also include the algorithms and other information;

d) Standardize the whole <SignedInfo> element, calculate its summary and the signature of the

summary, insert the value of signature to the <SignatureValue> element;
e) Add key information;
f) Put <SignedInfo>, <SignatureValue> and <KeyInfo> into the < Signature > element properly.

2) Verification of XML signature

The verification of XML digital signature Contains the below essential steps:
a) The signature confirmation: comparing the produced encryption abstract value with that in the <SignatureValue> element, if do not match, then signature confirmation defeat.
b) The quotation confirmation (Reference Validation): comparing the produced abstract value with that in the <DigestValue> element abstract value, if has any no match, then the quotation confirmation defeat, namely the primary data object is changed. Verification of the XML signature passes, only when all of the two steps above succeed

5. XML ENCRYPTION

5.1 Overview

XML Encryption is an encryption technology that is optimized for XML data. Its practical benefits include partial encryption, which encrypts specific tags contained in XML data, multiple encryption, which encrypts data multiple times, and complex encryption, such as the designation of recipients who were permitted to decrypt respective portions of data. The use of XML Encryption also helps solve security problems, including XML data eavesdropping.

5.2 Comparing with the traditional encryption

At present, transmission level secure TLS (transport layer security) is the fact standard of the secure communication on Internet. TLS is end-to-end secure agreement after the security sleeve joint character level (SSL), is one very safe and the reliable agreement, it has provided end-to-end secure conversation between both of the correspondence sides. In the traditional encryption, usually is the hypothesis that carries on the encryption to the entire definite orders with the single key.

The XML encryption (XML encryption) doesn't replace or substitute for SSL/TLS on the contrary, it provided the secure demand mechanism used for the SSL uncovering. The XML encryption process permits using many symmetrical keys or many asymmetrical keys to realize the element level encryption.

Traditional SSL/TLS doesn't t involve two domains in a part of encryption exchange data; secure conversation in every way. But the XML encryption standard may carry on the encryption to some parts selected of the documents, the user can only carry on the encryption to the important part which needs to protect. And, the XML encryption provides one kind of end-to-end security for application procedure which needed secure exchange of structured data.

5.3 Xml encryption syntax

This specification provides for encryption formats using XML and processing rules regarding encryption and decryption. **Figure 3** shows an XML encryption format and an example of XML-encrypted XML data.

As shown in Fig. 3, XML-encrypted data is of a document structure with the <EncryptedData> element at its top. Under the <EncryptedData> element, lie its child elements, including the <Encryption- Method> element, which contains information on the algorithm used for encryption, the <KeyInfo> element, which contains information on the decryption key to be used for decryption, and the <CipherData> element, which contains the cipher data. If hybrid encryption is used, the structure can also include the <EncryptedKey> element, which contains the key encryption key. In addition to XML signatures and in order to ensure that multiple encryption and designation of multiple recipients are possible URIs can also be used to specify what is to be encrypted. This feature enables users to build extremely flexible systems using XML Encryption [2].

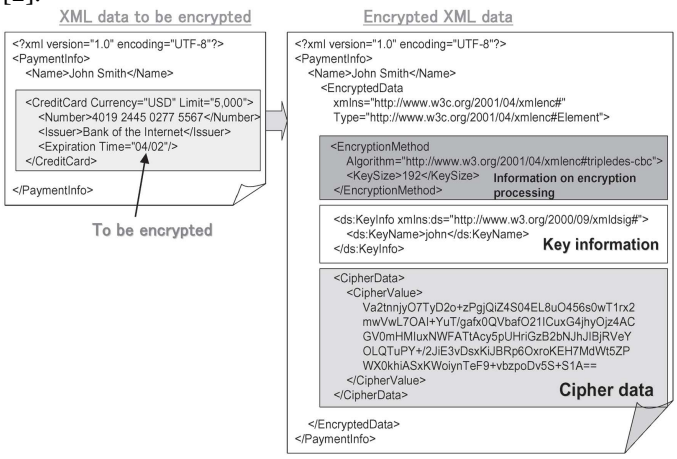

Fig. 3 XML encryption format example.

5.4 Steps of xml encryption

The XML encryption defined one process of producing cipher text for a clear text and recovery the clear text through decryption the cipher text [1].

1) Choice encryption algorithm

In the XML encryption algorithm, has the symmetrical encryption and the asymmetrical encryption, DES, AES and so on is the more popular symmetrical key algorithm at present, and RSA is the most widespread application asymmetrical key algorithm at present. The symmetrical encryption's speed of encrypts/ decipher is more quick, but how does the shared system key exchange mechanism

transmit the shared system key between mutual confidence both sides has its inherent flaw. Because of asymmetrical encryption and the symmetrical encryption algorithm has the respective shortcoming, then may unify them to use in the practical application. May use asymmetrical first encrypt the exchange symmetrical key, then uses the symmetrical encryption to exchange the XML data

2) Choice key transmission method

Decipher must use the key, may transmit the method of decipher key's ,doesn't transmit the key , use key name or other related information, encryption key after transmits. Suppose, now has A, B both sides to carry on the data exchange, simplified exchange model, as shown in figure 4.

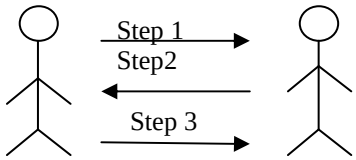

Fig. 4 Exchange model

The first step: A gives its public key by the XML document's to B; The second step: B use the public key encryption key transmitted by A to encrypt key, and reply for A by form of XML document (, because a private key of A only he knew, therefore encryption document only that A can decipher); The third step: A, B both sides mutually transmit the XML documents which has been encrypted with the key. After the second step, A, B both sides have the shared system key, both sides may use the shared encryption key to add/decipher the XML document, the third step is symmetrical encryption.

3) Encrypts the primary data, product the XML documents of encryption

The <EncryptedData> element is the most foundation element in the XML encryption syntax, included the position of the data pool waiting to encrypt, the encryption algorithm and so on.

6. CONCLUSION

The Web service is based on SOAP and WSDL standard agreement, and so on; they are to describe one kind of standard data and the message format expression by the XML format. For implementation of Web services security, the best is standard protocol based on opening, rather than rely on some proprietary format. XML signature and encryption specification integrates security into the XML environment. Its multiplicity makes it possible to design the security applications that spanning unit boundary and participate in every way, and its durability ensures that each participator can maintain a safe manner. XML signature and encryption technology has met the Web service security needs, which can be as the base of secure Web services.

7. REFERENCES

[1] "Web Services Security Based on XML Signature and XML Encryption", Gu Yue-sheng, Ye Meng-tao, Gan Yong, / JOURNAL OF NETWORKS, VOL. 5, NO. 9, SEPTEMBER 2010.

[2] "XML Signature/Encryption —the Basis of Web services Security" Koji MIYAUCHI / NEC Journal of Advanced Technology, Vol. 2, No. 1, pp. 35-39, January 2005.

[3] "Securing Web Services Using XML Signature and XML Encryption" RA. K. Saravanaguru, George Abraham, Krishnakumar Venkata subramanian, Kiransinh Borasia/ International Journal of Computer Applications, 2011

[4]" Secure Payment Information Using XML Technology", Ajeet Singh, Karan Singh, Shahazad, Azath M, Sathish Kumar Konga/IJARCSSE, Volume 2, Issue 5, May 2012

[5] E. Newcomer (2002). Understanding Web Services: XML, WSDL, SOAP, and UDDI. Addison Wesley. Yue-sheng, G., Bao-jian, Z. and Wu, X. (2009)

[6] 'Research and Realization of Web Service Security Based on XML Signature', In Proceedings of International Conference on National and Digital Security, pp. 116– 118

[7]Zheng Dongxi, Tang Shaohua, and Li shaofa, "XML Web services security technology overview", Computer Engineering and application, No.7, pp.38-41, July 2004

[8] Ma Hongliang, "Research and realization of Web Service safety technology based on XML", Dissertation of Xi'an University of Science and Technology, pp.6-32, 2007.

[9] Liu Cuiyin, and Liu Xia. "Research and application of the XML signature", *Computer applications and software*, Vol.24, No.4, pp.36-38, April 2007

[10]Singhal, A., Winograd, T. and Scarfone, K. (2007)'Guide to Secure Web Services', Recommendations of the National Institute of Standards and Technology. Special Publication 800-95