Web Services Security Based on XML Signature and XML Encryption

Gu Yue-sheng
Henan Institute of Science and Technology, Xinxiang, China
Email: hz34567@126.com

Ye Meng-tao
Henan Institute of Science and Technology, Xinxiang, China

Gan Yong
Zhenzhou University of Light Industry, Zhenzhou, China

Abstract—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. After analysis the traditional web services security technology, this 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, security, XML signature, verification, XML encryption, granularity

I. 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.

II. TRADITIONAL 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>
<thead>
<tr>
<th>TABLE I. PROTOCOL STACK OF WEB SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>UDDI</td>
</tr>
<tr>
<td>WSDL</td>
</tr>
<tr>
<td>SOAP</td>
</tr>
<tr>
<td>XML</td>
</tr>
<tr>
<td>HTTP FTP SMTP</td>
</tr>
</tbody>
</table>

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 ready-made 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. XML signature and encryption is developed by W3C and the IETF, 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, undeniability of XML document, and so on.

III XML SIGNATURES

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.

A. 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.

The XML signature standard supports for any digital content to carry on the digital signature, in the signature, signs apply in the digital content through the indirect way. First, carry on the abstract process and lay aside in a XML element the content which must sign. Then, carry on the abstract and the signature to this element. What XML signature represents is the XML element after signed, but is not the primary data. Abstract processing is the process of using the abstract algorithm (for example MD5, SHA-1 and so on) to calculate the hash value of primary data. The signature process is carrying on to this hash value. Because abstract value usually comparing to primary data is smaller many, therefore using it can be possible to reduce time of signing the data and use small space, thus causing transmission and memory of the data is more effective. The hash value is the “fingerprint” of primary data, any small modification to primary data, because of “the avalanche effect” of abstract algorithm, the hash value can have the huge change. After the hash value has signed, will guarantee the XML documents cannot change and the integrity of documents. Moreover, because carrying on the signature to the hash value is to use individual key, therefore simultaneously proves unsigned's status, namely identification authentication.

B. Comparing with the traditional digital signature

Compared 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 profit 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 <KeyValue> 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.

C. XML signature syntax

Table 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.

<table>
<thead>
<tr>
<th>TABLE II. XML SIGNATURE FORMAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Signature ID ?&gt;</td>
</tr>
<tr>
<td>&lt;SignedInfo&gt;</td>
</tr>
<tr>
<td>&lt;CanonicalizationMethod/&gt;</td>
</tr>
<tr>
<td>&lt;SignatureMethod/&gt;</td>
</tr>
<tr>
<td>(&lt;Reference URI ?&gt;</td>
</tr>
<tr>
<td>(&lt;Transorms/&gt;) ?</td>
</tr>
<tr>
<td>&lt;DigestMethod&gt;</td>
</tr>
<tr>
<td>&lt;DigestValue/&gt;</td>
</tr>
<tr>
<td>&lt;/DigestMethod&gt;</td>
</tr>
<tr>
<td>&lt;Reference &gt; +</td>
</tr>
<tr>
<td>&lt;/SignedInfo&gt;</td>
</tr>
<tr>
<td>&lt;SignatureValue/&gt;</td>
</tr>
<tr>
<td>(&lt;KeyInfo/&gt;?)</td>
</tr>
<tr>
<td>(&lt;Object ID ? /&gt;) *</td>
</tr>
<tr>
<td>&lt;/Signature&gt;</td>
</tr>
</tbody>
</table>

D. Formulation and verification of XML signature

5) 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.

6) 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.

E. Realization of XML signature

As a typical application, a whole program is shown below to produce and verify the XML signature.

1) Production of signature

KeyStore keystore=KeyStore.getInstance(“JKS”);
keystore.load(new FileInputStream(keystorepath),storepass);
X509Certificate cert=(X509Certificate)keystore.getCertificate(alias);
Key key= keystore.getKey(alias,keypass);
If (key==null) {System.err.println("Could not get a key,"+alias);System.exit();}
KeyInfo ekinfo=dsig.SignatureUtil.createKeyInfo(cert);
Element signatureElement=signatureGen.getSignatureElement();
keyinfo.insertTo(signatureElement,prefix);
signatureContext sigContext=new SignatureContext();
sigContext.setIdResolver(sig);
sigContext.sign(signatureElement,key);
doc.appendChild(signatureElement);
dsig.SignatureUtil.printDocum(do,System.out);

2) Verification of signature

XmlDocument xdoc=new XmlDocument();
xdoc.PreserveWhitespace=true;
XmlTextReader xfile=new XmlTextReader(filename);
xdoc.Load(xfile);
xfile.Close();
SignedXml sx=new SignedXml(xdoc);
XmlNodeList nl=xdoc.GetElementsByTagName(“Signature”,
“http://www.w3.org/2000/09/xmldsig#”);
sx.LoadXml(XElement nl[0]);
if (sx.CheckSignature())
{Console.WriteLine("Sign check Pass !");}
else
{ Console.WriteLine("Sign check Fail !");}

IV XML ENCRYPTIONS

The XML signature may realize the integrity of documents, and may carry on the identification authentication, but the documents also need the confidentiality.

A. 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 different part of XML 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, and documents after encryption is safe in status of transmitting and store status. In the XML encryption, data after the encryption indicates by the XML form, and marks by an element or <EncryptedData> element. The element is used to express all encryption content besides encryption key, but the<EncryptedKey> element is used to express that the data after encryption is an encryption key. Besides express encryption content, the XML encryption also express other encryption information, like use the encryption algorithm and the encryption key and so on, enable the work of the application procedure to simplify. Moreover, when XML encryption encrypt to XML documents, it has not defined any new encryption...
algorithm, but construct above the existing algorithm, thus causes interoperability possibly to become.

B. 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.

C. Steps of XML encryption

The XML encryption defined one process of producing a cipher text for a clear text and recovery the clear text through decryption the cipher text:

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 1.

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.

D. granularity of XML encryption

The basic granularity unit of XML encryption is an element. The encryption granularity may apply in three kinds of situations: (1) XML element encryption; (2) XML element content encryption; (3) random data encryption.

The element encryption is (including attribute) encrypts to the entire element, and uses the <EncryptedData> element to replace it. The content encryption only encrypts the sub node of element, and replaces it with the <EncryptedData> element. But the traditional encryption technology can only encrypt the entire documents, cannot carry on the selective encryption according to the demand to the documents. XML may also encrypt willfully other form data, may through by providing the IANA value to encrypt any form, only need to change the URI of <EncryptedData> element Type attribute.

Table 3 is an example of encrypting <CardId> content in the XML documents: The <EncryptedData> element has replaced <CardId> in the documents, other part of documents is invariable. Other element content after the encryption may be known for anybody, but the <CardId> element content only can be obtained by person has the related decipher key.

As table 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 <CipherData> element, which contains the cipher data. If hybrid encryption is used, the structure can also include the <EncryptedKey> element, which contains the 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.

![TABLE III. DEMONSTRATION OF XML ENCRYPTION]

<table>
<thead>
<tr>
<th>Original XML data:</th>
<th>&lt;?xml version='1.0'?&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;PaymentInfo xmlns='http://example.org/paymentv2'&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;Name&gt;John Smith&lt;/Name&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;CreditCard Limit='5,000' Currency='USD'&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;CardId&gt;4019244502775567&lt;/CardId&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;Issuer&gt;Bank of the Internet&lt;/Issuer&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;Expiration&gt;10/08&lt;/Expiration&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/CreditCard&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/PaymentInfo&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encrypted XML data:</th>
<th>&lt;?xml version='1.0'?&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;PaymentInfo xmlns='http://example.org/paymentv2'&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;Name&gt;John Smith&lt;/Name&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;CreditCard Limit='5,000' Currency='USD'&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;CardId &gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;EncryptedData xmlns='<a href="http://www.w3.org/2001/04/xmlenc#">http://www.w3.org/2001/04/xmlenc#</a>'</td>
</tr>
<tr>
<td></td>
<td>Type='<a href="http://www.w3.org/2001/04/xmlenc#Content'%3E">http://www.w3.org/2001/04/xmlenc#Content'&gt;</a></td>
</tr>
<tr>
<td></td>
<td>&lt;CipherData&gt;&lt;CipherValue&gt;A23B45C56&lt;/CipherValue&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/CipherData&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/EncryptedData&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/CardId &gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;Issuer&gt;Bank of the Internet&lt;/Issuer&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;Expiration&gt;10/08&lt;/Expiration&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/CreditCard&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/PaymentInfo&gt;</td>
</tr>
</tbody>
</table>

E. Decryption Transform for XML Signature

The Decryption Transform for XML Signature specification was established to solve problems that are raised when XML Signature and XML Encryption are used at the same time. It provides for a method used to determine whether XML encryption has been applied before or after the XML signature creation. This has been established by the W3C’s XML encryption working group as an additional specification with regard to the conversion processing that is performed on XML signatures.

F. Realization of XML encryption

As a typical application, a whole program is shown below to encrypt and decrypt the XML file.

1) Procedure of encryption

a) Creating a XmlDocument object, and loading the XML file that will be encrypted:

```
XmlDocument xdoc=new XmlDocument();
xdoc.Load("encrypting.xml");
```

b) Creating an EncryptedXml object, and transmitting the object of step (1) to it as a parameter:

```
EncryptedXml exml=new EncryptedXml(xdoc);
```

c) Getting the key by using the function GetNumberingKey(), and setting up the reflection between the key and its name:

```
RSA numberingKey=GetNumberingKey();
exml.AddKeyNameMapping("id", numberingKey);
```

d) Getting the element that will be encrypted:

```
XmlNodeList xnode=xdoc.GetElementsByTagName('cardid');
XmlElement xelement = XmlElement(xnode[0]);
```

e) Producing the encrypted data by using Encrypt method:

```
EncryptedData encryptedNeedEncrypt =
exml.Encrypt(xelement,"id");
```

f) Replacing the unencrypted part of the original XML file with the new encrypted data:

```
exml.ReplaceElement(xelement,encryptedNeedEncrypt,true);
```

Then, the encrypted XML file is produced.

2) Procedure of decryption

a) Loading the encrypted XML file:

```
XmlDocument xdoc = new

XmlDocument("encrypted.xml");
```

b) Setting up the reflection between the key and its name:

```
RSA numberingKey = GetNumberingKey();
exml.AddKeyNameMapping("numbering", numberingKey);
```

c) Decrypting the data by using DecryptDocument method:

```
exml.DecryptDocument();
```

Then, the decrypted XML file is produced.

V 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 participant 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.

REFERENCES

http://www.w3.org/TR/ws-arch/, W3C Working Group
Note 11 February 2004.

[2] D Eastlake, and J Reagle, “XML Signature Syntax and
Processing (2E)”, http://www.w3.org/TR/xmldsig-core/,
W3C Recommendation 10 June 2008.


Gu Yuesheng  a teacher of department of computer science in Henan Institute of Science and Technology, Xinxiang, China, Working in the area of computer network technology and application.