A Review On Various Message Security Services Using XML

Ankita Gandhi
Student of M.Tech, COE Department, SITE Nathdwara, Rajasthan, India

Asst. Prof. Ajay Dhabaria
Assistant Professor, COE Department, SITE Nathdwara, Rajasthan, India

Abstract

With the development of Web service application, some issues of web service security are increasingly prominent. XML is a Platform –independent Language which is used for to transfer data from one place to other place very much securely. This paper describes the review of how we will improve the security of message in Service Oriented Architecture through creating the web service. Here we formulate the XML Signature & encryption as the core of web service security technology & describe how to create & verify, how to encrypt or decrypt XML data. Mainly XML Encryption is used for provide security to message when it is stored in created web service.

Keywords: Web service, SOA, SOAP, XML Encryption, XML Certificate, XML Signature;

1. Introduction:

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 the security in using XML, especially the sensitive information described in XML, it can be handle With by combining with XML signature, XML certificate & encryption. The use of XML as core data syntax, the XML Encryption to protect confidential data— in the context of Web Services. The XML Encryption specification describes the process and syntax to be used when applying a cryptographic algorithm for data encryption to arbitrary XML-structured data. Moreover, it also describes how to process this syntax in order to decrypt the encrypted contents through web service. XML Encryption does not describe a new cryptographic algorithm itself, but merely allows a set of standard block ciphers, namely AES and Triple-DES (3DES). This paper also investigates the possibility of using the XML tree similarity based approach in order to individuate similar SOAP messages, that can be aggregated by the sender in a single message before applying WS-Security, which is a message security mechanism that uses XML Encryption and XML Digital Signature to secure web services messages sent over SOAP. A performance analysis and a comparison with other security mechanism are also presented.

2. Various Message Security Services :

According to the review of different research paper, SOA will have two requirements in the security area:

- Identity management service. The service mainly includes:
  a) Identity recognition verification.
  b) Identity authorization.
  c) Identity federation management and single logon.

Now overall survey of this paper is it introduce the end to end SOA Security service model and realize the dynamic and semantic security strategy management mechanism combining with the Semantic model. And it gives the future work related to prevent conflict which is occurring in message level end to end security.

- Message-level security: the confidential and privacy of the sensitive information must be protected during the exchange of sensitive information between the partners and probably by the safe way.

- Security strategy dynamic adjustment: security strategy can be update and execute dynamically according to the changes of context to realize web service security access intelligently.

From above three, we will go for the message level security. so, now, here we are describe the different requirement with it's specification for secure the message. Below table describe the same.

Dimension	Requirement	Specifications
Messaging	Confidentiality	WS-Security
		SSL/TLS
	Authentication	WS-Security Tokens
		SSL/TLS X.509 Certificates

Table:1 Secure WS Specifications and Standards Addressing

- Confidentiality: It is used to keep the information secret so that only intended recipient can read. Data confidentiality is accomplished by using security services i.e. encryption. With the help of encryption method, the data can be accessed only to the authorized parties. Here use openSSL tool to measure the integrity or confidentiality.[4]

- Authentication: It is used to establish or validate the identity throughout the system. Authentication is accomplished by using validation method. With the use of validation, one can access the secured system with username and/or password in an open e-Commerce system. This Paper Describe about the X.509 Certificate which is also used for authenticating.

Web Services Security is a message-level standard that is based on securing SOAP messages through XML digital signature, confidentiality through XML encryption, and credential propagation through security tokens. The Web services security specification defines the core facilities for protecting the integrity and confidentiality of a message and provided mechanisms for associating security-related claims with the message. In this part we will discuss some Security mechanisms of message Security services

Below figure 2.1. Describe the different message security services for improve the message security level in web service.

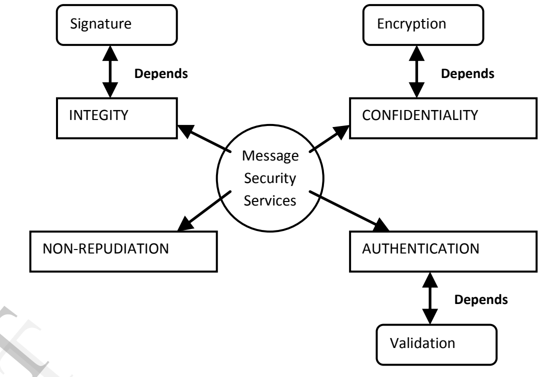

FIGURE: 2.1 Different Message Security Services

3. W3C XML Encryption:

XML encryption in W3C provides encryption for various sizes of units. The followings are the XML encryption units. [1]

- The whole XML document
- One element of XML document(and its children elements and attributes)
- One element value of XML document(and part or whole of its child nodes)
- The binary value outside of XML document

XML is the language of choice for a variety of reasons.
Main Features of XML is as

- XML is for structuring Data

- XML looks a bit like HTML
- XML is text but isn't meant to be read
- XML is verbose by design

- XML is a family of technologies
- XML leads XML to XHTML
- XML is modular
- XML is new but not that new
- XML is the basis for Resource Description Framework (RDF) and Semantic Web & also is license-free, platform-independent and well supported.

The XML Encryption recommendation defines an XML vocabulary and processing rules enabling confidentiality to be applied to a variety of content. XML Encryption serves the purpose of maintaining the confidentiality of information while in transit as well as when stored. And also preserve the data integrity between a message as a file before and after applying the XML- Encryption. In that also we have to apply different methodology. Like XML Data Structure, Odd-Even data Methodology, etc… using this we can apply any one methodology to improve the message.

4. XML Signature:

XML Signature is a technology that is optimized for XML data which is our message. The benefits of this technology, which allows a signature to be written on specific tags contained in XML data[3]. 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. What XML signature represents is the XML element after signed, but is not the primary data. After the verifying XML Signature the XML documents cannot change and the integrity of documents[5].XML Signature is used for provide the data integrity. In asp.net we can used the EnvelopedSignatureTransform () [2] to create a enveloped Signature & add it in to created reference object. And after that created signature is attached with the final encrypted document. In order for a document to be a valid XML, it must be well formed. Therefore, it is required to verify that the document is well formed prior to any other operation on it[7]. In accordance with the XML Signature Syntax and Processing specification a document must be well formed, and must have a canonicalization method that is applied prior to being passed through a function to compute the message digests.

5. XML Certificate:

XML certificate is used for improve the security level of message. The structure of an X.509 certificate is as follows: it includes the Certificate Name, Version, Serial No, and Validity etc…Now for Create a Certificate use makecert.exe (Certificate Creation Tool).

6. Conclusion:

This paper give the overview of different Message Security Services & overview of current security standards for XML and Web services. And also describes the different techniques to improve message security using Web services. XML encryption is new technology to achieve secure transmission of document which is considered as a Message. It described the Certificate-based XML encryption through a combination usage of different Security algorithms to create an encrypted XML that complies with W3C standard.

7. Future work:

In the future the proposed method will be applied on the XML Document to improve Message security in service oriented Architecture using web service.

8. References:

[1]XML Encryption Syntax and Processing (W3C Recommendation),2003.
[2]XML-Signature Syntax and Processing (W3C/IETF Recommendation), February -2002
[3]Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia and Ed Simon, “XML-Signature Syntax and Processing,” W3C Recommendation, Feb. 2002.
[4]D. Eastlake and J. Reagle, “XML Encryption Syntax and Processing,” W3C Recommendation 10 December 2003
[5]W3C.XML-Signature Syntax and Processing. February 12,2002.http://www.w3.org/TR/ xmldsig-core /.
[6]“Oasis security services (saml) tc,” ”http://www.oasisopen. org/committees/security/”.
[7]Merlin Hughes, Takeshi Imamura, Hiroshi Maruyama, “Decryption Transform for XML Signature”, W3C Recommendation 10 December 2002. URL=http://www.w3.org/TR/xmlenc-decrypt/
[8] Philippe Camacho, “An Introduction to XML Signature and XML Encryption with XMLSec”, URL=http://www.dcc.uchile.cl/~pcamacho/tutorial/web/xmlsec/xmlsec.html