Web Services Security based on XML Signature & XML Encryption

John Mathew[1] Hari R[2] Prof. Govinda K[3]

[1,2,3] VIT University, Vellore, Tamil Nadu-632014, India

Abstract— The web services applications were developed to a large extend and the issues regarding web service security are becoming increasingly prominent. Since the XML is a platform independent language, and has high expandability, it is widely used in deploying web service applications. Therefore it is necessary to consider adding some security features in XML document. The security features like access control, digital signature and element-wise encryption cannot be implemented using transport layer security protocol such as Transport Layer Security (TLS) or Secure Socket Layer (SSL). SSL is a reliable and secure protocol which provides end-to-end security sessions between two parties. The XML Encryption is not a replacement to the SSL. But, XML Encryption is used to provide security features that are not addressed by the SSL. For example, with XML Encryption both insecure and secure contents can be exchanged between multiple parties. This paper discusses about the use of XML Encryption and XML Digital Signature as the core of web services security technology. The paper also describes the creation and verification of XML signature and encryption and decryption of XML data. The application of XML encryption and XML digital signature is also illustrated here.

Keywords: Web Services, Security, XML Signature, XML encryption, SOAP, SSL

I. INTRODUCTION

Web Services which are widely used in current distributed systems forms the back bone of IT industry. Most of the business transactions across the internet rely on Web Services for achieving the goals. XML which stands for extensible mark-up language adds portability and customizability which in turn results in better business communication. The interface for web service is described in WSDL and communication is performed using SOAP messages [2]. Since the demand for Web Service is increasing, reliability and security among applications and communication between the applications should be maintained. Web Service security depends on integrity, confidentiality of SOAP messages as well as the security of service itself. Organizations such as OASIS and World Wide Web Consortium have been focusing on XML and Web Service Security for the past few years. As a result they have standardized the specifications of Web Services.

According to the survey done by an US company called Evans Data Corporation about 40% of the web developers' use web services. Another survey conducted by Dixit states that 82% of the respondents' uses Web services for their existing applications and about 18% of the survey respondents showed interest in fully featured implementation of Web Services for future applications. It was also noted that there occurred a great increase in Web Service expenditure, although the current market trends were against the development. Lange (2003) clearly predicted that there would me a mass rise in Web Service Expenditure from $1.2 billion to $21 billion in the time span of 2003 to 2007. IBM developers Works (2003a) provided a definition for Web Services as the programs which make use of Internet or intranet for accepting XML requests through lightweight, vendor-neutral communication protocols. A Web Service usually implemented by starting a remote procedure call where the application calls the remote program with arguments. SOAP which stands for Simple Object Access Protocol acts as the vendor-neutral protocol for the Web Service. SOAP message which contains XML describes all the necessary information related to the content [2]. Upon receiving the SOAP message application does its job and sends the result back in XML format.

SOAP messages are crucial for Web Service communications where integrity and confidentiality were provided along with information. Currently end to end security is being provided by the lower end layer protocols such as SSL/TLS. Since SOAP messages are often subjected to constant processing and modifications such as inserting and removal of SOAP header the above described protocols may be insufficient. Also the presence of different network protocols makes it insufficient for a lower layer mechanism such as TLS/SSL.

XML level security provides confidentiality and integrity at the source node and at the place of storage node.XML level security makes use of XML Encryption and XML Digital signature for providing security with the aid of powerful encryption algorithms such as RSA, SHA-1 and MD5.

This paper describes an overview of Web Security, Web Security Architecture, and various mechanisms for Web Security. Detailed description about the existing work is described next XML encryption in the next phase describe XML Signature and its various types and how to syntactically represent it. The remaining part deals with XML signature and its effective implement in Web Service environment.

II. LITERATURE SURVEY

XML Signature was the first W3C recommendation for security where signing of documents using digital signature was provided. Later XML Encryption with the use of algorithms provides integrity, authentication and non-repudiation evolved. Both provide partial as well as multiple signature or encryption.

Lautenbach (2004), [3] talks about XML Security Standards and its needs in his paper. He states that signing or encrypting an XML document is similar to an ordinary document where the problem arises are the changes by parsing, changes by serialization, changes in character sets, inability to represent `signature value or output in XML format. He describes XML Security, XML Encryption their

syntaxes and processing rules and also XML Canonicalization and granularization He also describes XPath Filter 2 Transform, XML Key management specification, Security assertion markup language in his paper.

Yue-sheng, Meng-tao and Yao (2010), describes the need of XML Encryption and XML Signatures in Web Security. They pointed out that the current SSL cannot meet the web service security. In the paper it is described that how xml signature verification can be done and how web services based on SOAP and WSDL can be made secure as they are based on XML standards.

Bertino, Carminati and Ferrari (2001), [6] states the authenticity, integrity in XML security and the need of access control mechanisms as well as the need of XML Signature or XML Encryption in their paper. They talks about Author-X a java based system developed for providing security in XML documents. They also describe Secure XML publishing where digital signatures can be used for providing security which ensures authenticity and confidentiality in publishers' point of view.

Nordbotten (2009), [5] in his paper, describes the current XML standards which provide security in terms of confidentiality, integrity and authentication. He describes WS Security for SOAP messages, Web Services policy and WS-Trust where augmentation of WS-Policy and WS-Security for multiple message exchanges. A description about XML Key Management Specification as well as description about various languages like extensible Access Markup Language and Security Assertion Markup Language was included in his paper.

Yue-sheng, Bao-jian and Wu (2009), [8] talks about the limitations of SSL which was one of the traditional security standard where point to point security is ensured.XML Syntax and processing was described in the later section followed by java implementation of XML Signature in Web Service Security.

Sun and Li (2005) and Han,[5] Park and Lim (2011), [9] in their paper describes the benefits of XML Signature, the use of undeniable XML Signature with the aid of RSA encryption. Undeniable Signature ensures the signer's validation for verifying the document. They also discuss the common ecommerce frameworks and its security. In addition they discuss about the XML Signature, types, verification and application for the use in ecommerce environment.

Takase and Uramoto (2002) and Knap and Mlynkova (2009), in their paper describes the B2B communications and the use of XML Signature in them. They discussed in detail about the various security attacks existing in Web Service environment such as XML injection, denial of services and counterfeit in XML documents. Takase and Uramoto, in their paper proposed and described a proxy server using XML Digital Signature where it can be implemented as a Web Service.

III. WEB SERVICES SECURITY

The Web Services are dependent on the basic World Wide Web architecture and HTTP transport protocol, like normal web applications. So the web services are prone to vulnerabilities and security threats. In order to add security to the web services a feature-rich and flexible extension to the SOAP (Simple Object Access Protocol) known as Web Service Security in short WS-Security is established. The WS-Security is published by OASIS and is a part of the web services specification family.

The WS-Security is based on following security concepts:

- Confidentiality: Confidentiality is limiting the access to information and preventing disclosure of information to unauthorized users.
- Identification and Authentication: The process of verifying the identity of the user and the process of ensuring whether a user is who he or she claims to be.
- Authorization: The authorization provides permission to a user to access a resource based on his or her identity.
- Privacy: Privacy restricts the access of information by relying party or subscriber according to the Organizational Policy and Federal Law.
- Integrity: Integrity is ensuring that the information has not been modified by unauthorized users while transmitting.
- Non-Repudiation: Non-Repudiation refers to the ability to ensure that a service cannot be denied by either sender or receiver or any other third person.

A. Web Service Security Architecture

The Web Services were created by an open community. Many security standards were developed by the same open community. The WS-Security Architecture [6] showed in Figure 1 maps the security standards to the layers of the standard web service.

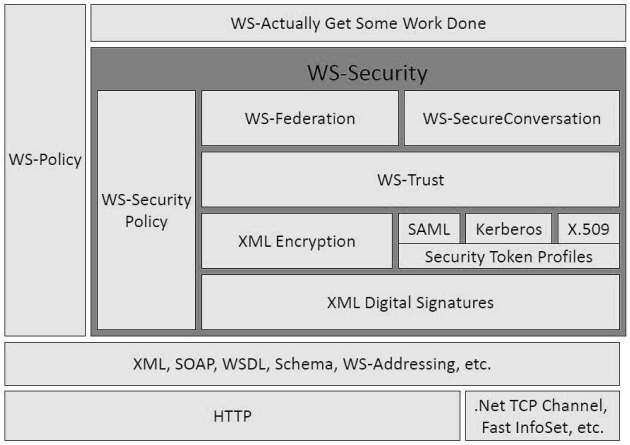

Fig. 1: Web Service Security Architecture.

The components of WS-Security Architecture [6] are described as follows.

- WS-Trust: The WS-Trust is a standard which is used to authenticate clients based on a centralized security server which is a security token service. The authenticated clients are issued with tokens which contains different kind of authorization and authentication data.

- WS-Policy: The WS-Policy describes the constraints and capabilities of the security policies applied on the endpoints and intermediaries in a network.
- WS-Privacy: The WS-Privacy is used to describe a model for how the Web Services and Web Services requesters' state organizational privacy practice statements and privacy preferences.
- WS-Security: The WS-Security is used to describe encryption and signatures headers can be attached to SOAP messages.
- WS-Federation: The WS-Federation describes the management of trust relationships in a federated heterogeneous environment.
- WS-Secure Conversation: The WS-Secure Conversation describes the authentication and management of message exchanges between parties. These include establishing and deriving session keys and security context exchange.

The XML Encryption and XML Signature are two standards for XML Security. This paper discuss about the basic concepts and implementation techniques used for XML Signature and XML Encryption.

IV. XML ENCRYPTION

The process that converts sensitive document into a understandable format to the unauthorized users is called Encryption. The converted document is known as Ciphered Data or Cipher Text. In order to understand the content the cipher text should be decrypted by the authorized users. Encryption is a technique that has been used for many years to maintain confidentiality. Public Key (Asymmetric Key) Encryption and Private Key (Symmetric Key) Encryption are two standards of encryption. These encryption standards can be used to encrypt XML document also.

XML Encryption is the process of encrypting xml data using the encryption standards. XML Encryption is released on December of 2002 and it is recommended by W3C. XML Encryption technology is optimized for xml data. XML Encryption allows multiple encryptions of data where data is encrypted several times, partial encryption where the encryption of particular tags contained in the xml file is done and complex encryption where different portions of data can be encrypted in such a way that different portions can be decrypted only by respective designated persons.

Following is a specifications established by W3C for XML Encryption.

A. Syntax of XML Encryption and Processing

In XML Encryption the encrypted data also follows XML syntax. Certain xml elements are added to the xml document to represent the encryption method, encrypted data etc. The XML encryption syntax is shown in Figure 2.

The XML encryption or Encrypted Information part in the xml document is represented by EncryptedData element. The Id, Type, MimeType and encoding are the attributes of EncryptedData element. The symbol "?" specifies one or zero occurrence, "*" denotes zero or more occurrences and the symbol "+" specifies one or more occurrence of the element or attribute. EncryptionMethod element is used to specify the algorithm used for encryption and the key size. The key size is specified as sub element and algorithm is specified as attribute of EncryptionMethod element.The KeyInfo element denotes the information about keying material that has to be used at recipient's side for decrypting the cipher data.

```
<EncryptedData Id? Type? MimeType? Encoding?>
  <EncryptionMethod/>?
  <ds:KeyInfo>
    <EncryptedKey>?
    <AgreementMethod>?
    <ds:KeyName>?
    <ds:RetrievalMethod>?
    <ds:*>?
  </ds:KeyInfo>?
  <CipherData>
    <CipherValue>?
    <CipherReference URI?>?
  </CipherData>
  <EncryptionProperties>?
</EncryptedData>
```

Fig. 2: Syntax of XML Encryption

The encrypted value is contained in CipherValue element which is a sub element of CipherData element. The CipherData element may contain CipherValue which is the actual cipher text or CipherReference element which is used to specify the reference to the cipher text.

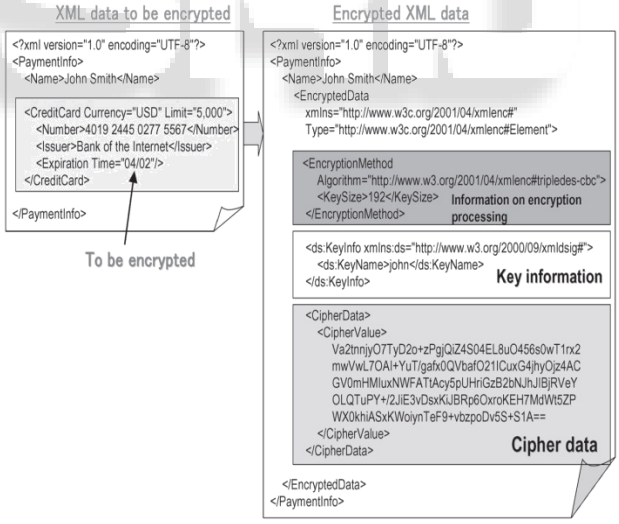

Fig. 3: Example of XML Encryption.

V. XML DIGITAL SIGNATURE

Digital Signatures which were key to electronic security provides non-repudiation of data, integrity of data and authenticity of data.XML Signature uses digital signature for the process of signing or verification of XML document. This standard was provided by W3C in the year 2002.XML signature allows additional features that normal SSL/TLS can provide. This includes partial signature where specific tags alone can be signed and Multiple Signature where multiple tags can be signed. Major Advantage of using these

specifications was that it can avoid falsification and spoofing.

The XML Signature allows encryption using Digital Signatures through any possible encryption algorithms.

Hash values which are called fingerprint of primary data are used in signing the document. A small change in primary data causes large alterations in hash value which allows providing enough security to the document. SHA-1, MD5 can be used for calculating hash values.

A. Types of XML Digital Signature

Basically there are three types of signatures provided. Enveloped Signature is a type of XML Digital Signature where Signature is embedded within the document and was the child of object being signed. Signed data envelopes the <signature> and </signature> tags. Figure 4 describes the format of XML Enveloped Signature. Enveloping Signature which was shown in Figure 5 describes how document can be included as child element of Signature element. Data being signed was written similar to Enveloped Signature. Figure 6 describes Detached Signature where signed XML Document as well as XML signature was separate documents. Usually non XML format was used for XML Signature document. Reference was provided inside the Signature element so that document can be easily accessed.

```
<document>
      …… Data
   <signature>
     …… Contains
     reference to   the
     Data being signed
   </signature>
</document>
```

Fig. 4: Enveloped XML Signature.

```
<signature>
      …… Contains
      reference to the
      signed data
</signature>
```

Fig. 5: Detached XML Signature.

```
<signature>
      …… Contains
      reference to the
      Data being signed
   <document>
      …… Data
   </document>
</signature>
```

Fig. 6: Enveloping XML Signature.

```
<signature>
      …… Contains
      reference to the
      signed data
</signature>
```

Fig. 7: Detached XML Signature.

B. XML Signature Structure

Signature element describes the structure of XML digital Signatures. Figure 7 shows the XML signature structure which was recommended by W3C. Use of "?" indicates that there can be zero or one occurrence, "+" indicates one or more occurrence and "*" indicates zero ore more occurrence. Below are the main information's an XML Signature should contain.

- Signed Info
- SignatureMethod inside Signature element describes the algorithm used for encryption. CanonicalizationMethod provides algorithm for the normalization of SignedInfo element. Reference element specifies the hashed XML fragment and Transforms element specifies set of transforms used in XML fragment. DigestMethod element specifies the hash function or method used for performing hash on the primary data and the result of hashing is stored inside DigestValue element.
- SignatureValue
- Signature value describes the result of the CanonicalizationMethod element which performs signing based on the parameters specified by the SignatureMethod element.
- KeyInfo
- This element describes the keys that can be used for validating the signature which was given by the signer**.** Usually this comes as an optional element in Signature element. X.509 digital certificates are used for providing the key details.

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

Fig. 7: XML Signature Structure.

C. Decryption Transform for XML Signature

When XML Encryption and XML Digital Signature are used together, it leads to some compatibility problems. In order to solve these problems a specification called Decryption Transform for XML Signature is used. The specification is used to identify whether xml digital signature is created after or before the xml encryption is done. The Description Transform for XML Signature specification was established by the W3C xml encryption working group for the processing of xml digital signatures.

VI. CONCLUSION

XML Encryption provides confidentiality and authorization where only the person who is intended to receive from the sender is able to extract the contents in the document.XML Signature provides integrity where document was received as such where no intermediate person was able to modify the document. Digital certificates are used for signing the document whereas algorithms such as RSA, SHA-1 can used for encryption. Authentication (Bertino, Carminati and Ferrari, 2001; Han, Park and Lim, 2011; Singhal, Winograd and Scarfone, 2007) enables server and client to ensure that the document is accessed by the right entity. Verification (Singhal, Winograd and Scarfone, 2007) was provided by both Encryption and Signature where decryption can be done by private key of receiver and public key of sender provides right sender. Integrity (Bertino, Carminati and Ferrari, 2001; Han, Park and Lim, 2011) ensures that information can be accessed or manipulated by the authorized only. Confidentiality (Bertino, Carminati and Ferrari, 2001; Han, Park and Lim, 2011) was provided by XML Encryption were data is described as cipher text instead of plain text. Non-Repudiation (Han, Park and Lim, 2011; Nordbotten, 2009; Singhal, Winograd and Scarfone, 2007) is to ensure that sender and receiver cannot deny later that he/she hasn't send the document. First sign and then encryption allows changing algorithm later without altering the signature. First encryption and then sign allows finding tampered data quickly.

REFERENCES

[1] Knap, T. and Mlynkova, I., 'Towards More Secure Web Services – Exploiting and Analysing XML Signature Security Issues', In Proceedings of 3rd International Conference on Research Challenges in Information Science, 2004.
[2] P. Hallam-Baker and S. H. Mysore, "XML Key Management Specification (XKMS 2.0)," W3C Recommendation, 2005.
[3] Lautenbach, B., 'Introduction to XML Encryption and XML Signature', Elsevier, pp. 6 – 18, 2004.
[4] Nordbotten, N. A., 'XML and Web Services Security Standards', IEEE Communications Survey and Tutorials, Vol. 11, No. 3, pp. 4 – 21, 2009.
[5] D. Booth, H. Haas, F. McCabe, E. Newcomer, C. Ferris, and D. Orchard. "Web Services Architecture," W3C Working Group Note, 2004.
[6] F. Curbera, M. Duftler, R. Khalaf, W. Nagy, N. Mukhi, and S. Weerawarana, "Unraveling the Web Services Web: An Introduction to SOAP, WSDL, and UDDI," IEEE Internet Comput., vol. 6, no. 1, 2002, pp. 86- 93.
[7] D. Eastlake, J. Reagle, D. Solo, F. Hirsch, and T. Roessler, "XML Signature Syntax and Processing (Second Edition)," W3C Recommendation, 2008.
[8] D. Eastlake and J. Reagle, "XML Encryption Syntax and Processing," W3C Recommendation, 2002.

