Literature Paper for Digital Signature based secure XML emails

Arekar Srushti, Jagtap Prajakta, Jagtap Priyanka, Sharanya Shivakumar

Abstract: XML has become the prime standards for data exchange on web and uniform data model for data integration. In the case of XML data, digital signature operation is applied to it, which is nothing but XML Digital Signature. It is a standard that is defined for signing an XML document and for representing a digital signature in an XML format. The use of XML format in the email system ensures security and privacy in its transaction. A higher level of security can be provided to the Digital Signature of our XML data by using XML Encryption. It is a flexible methodology for representing encrypted data in XML format. XML encryption supports the signing of the whole document or the partial document.

Keywords: XML security, XML encryption, XML signature, XML key management, Web services, XML decryption, XML retrieval

1. INTRODUCTION:

The drastic development of networked electronic mail (email) has been one of the major technical and sociological developments of the past 40 years. The Email system application functions with the help of Internet. The system is useful to all the general users, companies, big organizations to send the important documents, messages from one place to another, from one user to another. User's location does not matter in this application.

PGP and S/MIME are the most widely used mechanisms which provide following functionalities like non-repudiation, data integrity, data confidentiality. But it provides security only to the body of message and headers remain unauthenticated. These shortcomings can be overcome by two ways viz. by using XML format or by using Digital signature. A digital signature is a methodology which is used for securing the data using private and public key of user. Whereas XML format provides the markup structure for storing the data so that any changes in format of data do not affect the semantics of document

2. XML AND WEB SERVICE STANDARDS:

Web service is a method of communication between two electronic devices over World Wide Web. A web services is a software 6i0i/function provided at a network address over web or cloud. WSDL describes the web services and also about the way to access them.

Web service is a software system designed to support the interoperability of machine-to-machine interaction over a network. Web services work independent of the programming language and operating system. It is widely used in current distributed system and has become the technology of choice for implementing service oriented architecture (SOA).

Web services are in many ways combined with the XML. The heterogeneous integration of web service for various systems is facilitated through the use of XML. The interface of web service is a described using web service description language (WSDL) which is XML based. Even the communication is performed using XML based SOAP message. Thus, the web services are making it more secure for XML based system.

The conceptual relationship between the XML and web services standards are:

XML
XML Encryption
XML Signature
WS – Security
WS – Trust
WS Secure Conversation
Web Service Policies
Security markup language

1. XML:

The XML security standards define XML vocabularies and the processing rules in order to meet security requirements. It uses the cryptographic and security technologies to provide flexible and extensible solution satisfying security requirements.

2. XML Encryption:

Encryption of an XML document is similar to encrypting or signing any other document. Any encryption program can encrypt or sign an XML document. But this approach does not use the full capability of XML. There are some problems with this approach:

Normal signatures cannot handle the changes that occur due to parsing and reserialization. Also it is unable to handle changes made in the character sets.

There is inability to easily represent the value of a signature or the output of an encrypted XML document in XML format.

The best way to combat this problem is encrypting into binary data. When the encryption is done the output is a random stream of bits. When an XML file is encrypted the result is a set of binary bits which cannot be easily decrypted. Ideally, the encrypted XML file should also be in XML format so that it can be analyzed using the basic tools as the original file.

The standard XML encryption defines how to encrypt the XML documents.

Encryption is basically of two types:

1. Symmetric /secret Encryption:

In this situation sender and receiver share same secret key that is used to encrypt /decrypt messages.

2. Asymmetric/Public Key Encryption:

In this receiver publishes his public key which allows any sender to encrypt messages only receiver can decrypt message using private key.

XML encryption consist of three major parts-
Granularity
Syntax
Processing Rules

1. **Granularity:** Deals with data to be encrypted
2. **Syntax:** Gives format for representing encryption.
3. **Processing rules:** Defines series of action for encryption and decryption of xml documents.

3. XML signature:

XML signature provides XML syntax for digital signature which is used for signing documents of any type especially XML.

Canonical XML is especially important when it refers to XML signature, which guarantees, that logically identical XML documents create identical digital signature (for signing <signedinfo> canonicallization is mandatory). XML format consist of <SignedInfo>, <signaturevalue> and <keyinfo> elements.

And for checking validate signature <signedinfo> compared with <reference>.If both are matched indicates valid data.

4. WS – Security:

Web service security is extension to SOAP to apply security to web services. WS security deals with three major jobs:

Methods of signing SOAP messages to assure integrity.

Methods to encrypt SOAP messages to assure confidentiality.

Attachments of security tokens for identification of senders.

This protocol allows communication in format of Security Assertion Markup Language (SAML).

5. WS – Trust:

It is a WS-specification & OASIS
Standards that provides extension to WS-Security, dealing with issuing , validating of security tokens as well as way to establish access and broker trust relationship between participants in a secure message exchange. WS-trust specification authorized by number of companies and was approved by OASIS in 2007. WS-trust defines a number of new elements, concepts and artifacts in support of that goal. The concept of security token service that issues security token as defined in WS-Security specification. The format of message used to request security tokens and response to their message. Web service framework that implements WS- trust protocol for token request includes: Microsoft's Windows Communication Foundation (WCF) and Windows Identity Foundation (WIF).

6. WS-Secure Conversation:

It is web service specification which works with WS-Security, WS- trust and WS-policy to allow the creation and sharing of security context extending use of cases of WS-security. The purpose of WS-Conversation is to establish security context for multiple SOAP message exchange reducing overhead of key. It establishes a new security context.

Security context token created by security token service. Security context token created by one of the communicating parties and propagated with message. Security context token created through negotiation.

7. WS- Policies:

Web policies include a set of mandates or constraints, legal; compliance related that limits a company's online behavior. Company needs policy to enable responsible, appropriate decision making at all level of organization that is compliance with relevant.

8. Security Markup Languages:

A. XACML (Extensible Access Control Markup)
It defines declarative access control policy language implemented in XML and processing how to evaluate access request according to rules defined in policy. XACML model supports and encourage separation of access decision from point of use. When access decision baked into client application (or based on local machine, user ids and access control list (ACLS)) it is very difficult to update decision criteria when governing policy changes. When client is decoupled from access, authorization policies can be updated on fly and affect all client immediately.

B. SAML (Security Assertion Markup Language)
It is an OASIS open standard for representing and exchanging user identity and authentication data between parties. It provides web based single sign capability. With SAML a user can login to one system in an environment and then will be able to access to other system in that environment without needing to login again. Entities involved in SAML web browsers are:
Identity provider(IDP)
Service Provider(SP)
Principle(usually an end user)

Identity Provider maintains directory of users and all authentication mechanism to authenticate them.

Service provider target application that user tries to use. Assertion contain statement that service provider use for access control decision.

SAML consists of:

Authentication Assertion- the assertion subject was authenticated at a given time via an authentication mechanism.
Attribute Assertion- assertion subject is associated with the supplied attributes.
Authorize Decision- a request to allow assertion subject to access specified resources has been granted or refused.

XML Retrieval:

XML retrieval is a method of retrieving content of documents structured in XML. Base of this XML retrieval is Information retrieval (IR). Information retrieval concept includes ranking of similarity based search, and profile based search can be applied to XML query languages. XML retrieval supports multimedia fragment retrieval.

This consists of:

Motivation – It provides introduction of historical view of DB and IR communities.
Data model and queries – Data model is concerned with XML standards, basic Queering XML content, dealing with content and structure.
Effectiveness and efficiency: Ranking algorithm, document preprocessing indexing is done during process.
Evaluation – It is describing document collections, topic tasks and metrics.

Digital signature:

Digital code (generated and authenticated by a public key encryption) which when attached to an electronically transmitted document verifies its contents and sender's identity.

Need of Digital Signature:

Digital signature commonly used for software distribution, financial transaction.
It provides non- repudiation i.e. signer cannot claim that they did not sign the message.

Building blocks of Digital Signature are:

Private key: known to signer only
Public key: global key
Hash function: it is an algorithm to create unique message and document.

Property of authentication system:

highly secure
highly easy to use
low failure to authentication
low false acceptance rate
low false rejection rate

Digital Signature formation procedure:

Using hashing algorithm electronic document digest value calculated.
Private Key of the sender added to the digest value which results in electronic signature.

Digital Signature verification process:

Applying reverse hashing check whether digital signature that was created at the sender side matches with encrypted data using public key of transmitter.

Traditional authentication system:

Key Cards: Limited storage capabilities
Face reorganization: Lack of reliability
Retina Geometry: Lack of discriminative capacities
Retina scan: ineffectual with blind people

Year	Status
10/06/2008	XML syntax and processing (2nd Edition) Specifies XML signature “Decryption Transform” that enable xml Signature application to distinguish between those xml encryption structure that were encrypted before signing for signature to validate.
8/11/2012	XML signature Xpath filter 2.0
11/4/2013	XML signature syntax and processing version 1.1
11/4/2013	XML signature properties
11/4/2013	XML signature best practices
11/4/2013	XML signature syntax and processing
11/4/2013	XML security requirement and design consideration
18/6/2014	Test case for canonical XML 2.0

Table -1: Status in the field of XML signature

Conclusion:

In this paper, the system proposed by us takes the advantages of the XML, web services and XML digital signature. The XML Email provides us with the code which is efficient for processing, archiving and searching. This was possible due to the strong structure of XML. We have made sure about a secure end to end authentication with the help of XML encryption. XML signature has been used for the purpose of signing required data on the partial document by different parties. We have understood process of transportation that take place in an email system. We are efficiently using web services which make our system easy to use, secure and accessible.

Our system provides better counter measures against spam mails as we are able to track down source of email. The proposed system well verify sender and only then the email sent will be decrypted .Foreseeing many issues of spamming and hacking of current system ,our system fights back all these problems to provide privacy to both receiver and sender as well as security to email system.

ACKNOWLEDGMENT:

We were guided by Prof. Mrs. Anjali Kadam, assistant professor of Computer Department in Bharati Vidyapeeth College of Engineering for Women.

Our sincere thanks for her support and guidance. Her knowledge and support in the field of XML and web services was of great help in making our literature paper.

REFERENCES:

[1] Nils Agne Nordbotten, “XML and Web Services Security Standards”, IEEE communications surveys & tutorials, vol. 11, no. 3, third quarter ,2009.

[2] Berin Lautenbach, “Introduction to XML Encryption and XML Signature”, Information Security Technical Report. Vol. 9, No. 3, 2004.

[3] Digital Signature with Hashing and XML Signature Patterns.

[4] Understanding the limitations of S/MIME digital signatures for E-mails: A GUI based approach.

[5] Alok Gupta, Y. Alex Tung, James R. Marsden , “Digital signature: use and modification to achieve success in next generational e-business processes ”,Department of Information and Decision Sciences, Carlson School of Management, University of Minnesota, Minneapolis, MN 55455, USA, Department of Operations and Information Management, School of Business Administration, University of Connecticut, Storrs, CT 06269, USA ,Received 1 February 2002; received in revised form 1 February 2003; accepted 1 June 2003.

[6] Konstantin Beznosov , Donald J. Flinn , Shirley Kawamoto , Bret Hartman, “Introduction to Web services and their security” , Information Security Technical Report (2005).