International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 5, May - 2013

A Comprehensive Analysis Of Xml Digital Signature, Xml Encryption And Xkms

Rohit Ramesh And Subham Khandelwal
SCSE, VIT University, Vellore.

ABSTRACT- *The continuous involvement of w3c in improving XML security has led to numerous fruitful results. Authentication, Integrity and Privacy are indispensable terms in the field of security. Proliferating the standards of these three services will curtail any security related issues. This paper's main objective is to elaborate different approaches to neutralize security threats. The three primitive methods to create a protected environment in XML are namely: XML Signature, XML Encryption and XKMS (XML Key Management Specification). In our paper we have analyzed the usage strategies of the above-mentioned methods, which will tackle adverse circumstances like- forgery, unauthorized access to valuable data etc.*

I. INTRODUCTION

A web system is defined as a software, which supports inter, or intra machine-to-machine communication over a standard network. These services are widely used in distributed system architectures and have slowly become the principal choice for service-oriented architecture. They provide a cavity for independent programming and operating systems [1]. The Internet is a rapidly developing phenomenon and its influence in our daily lives cannot be stressed enough. Thus it is very important that we exploit it to the fullest. This exploitation also means that we make it secure [2]. Just like in other information systems, the reliability and security of the system could be addressed in various ways right from technical measures to legislative measures [3].

XML or Extensible Markup Language is a language defining a conglomeration of rules structured to create a human and machine-readable language. Simplicity and easy usability are the main advantages of XML. XML is principally a scheme of describing data in formats that makes it accessible to application no matter what format it is expected in. Its versatility in this regard is unparalleled.

Security in web systems can be achieved by XML's security mechanisms. The two major issues that need to be addressed are, predominantly restricting access to a XML Web service to unauthorized users or elements which aim to exploit its services for unethical motives and to preserve the confidentiality and integrity of the XML component [12]. Authentication and Privacy are vital for any user who uses web systems. To help achieve these features we use XML security as a benchmark. XML security can be classified into two cardinal access controls; the server access control and the sub tree encryption.

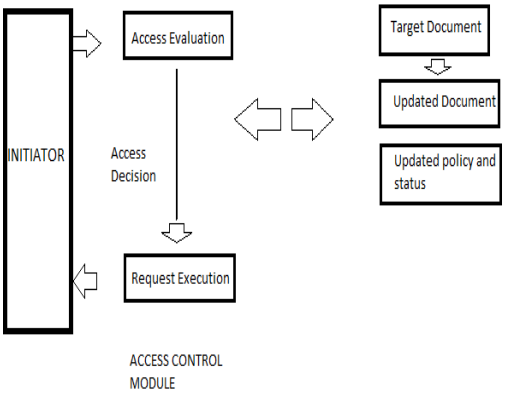

Fig.1. Access Control Model [13].

In the server access control the XML document is present on a server. When it is requested by a client it is authenticated, authorized and verified. In most of the cases these authorizations are elaborated. The accessibility of the element nodes of the document is hence defined. Sub tree

encryption is an element wise encryption i.e. the encrypted document defines the process for encryption of data and the result in XML. The data may be classified to be the content of an XML element or the XML element itself [7]. XML security simplifies adoption by defining minimum mechanisms or processes to obtain powerful or maximum results. By applying existing paradigms and tools XML curtails the need to modify submission to meet security standards [8].

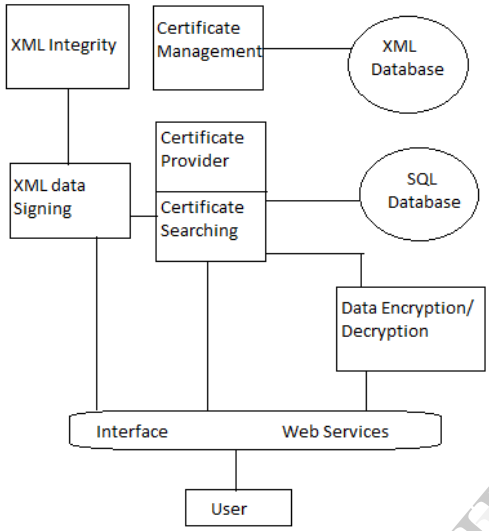

Fig.2. XML Architecture [4].

In this paper we discuss in detail about XML Signature, XML Encryption and XKMS (XML Key Management Specification).

II. Digital Signature

XML digital signature is similar to the digital signature mechanism employed in standard encryption and decryption mechanism. It is optimized for signing XML data. XML digital Signature has a special feature where multiple tags can be signed in the XML base. This digital signature was developed to solve wide spread problems like spoofing, phishing and other misuse of social enterprise systems. The XML digital Signature is stored in <signature> element and its result is represented by a string of code which can be derived from the input data. A third party who would act as a certificate authority may be included in the mechanism. These signatures are used extensively in network communications. This whole process is embedded in network resources, thus making it more networks efficient. Some of the other elements used are:

- **<signedinfo>** - Defines References to the algorithm used to create the signature. It also stores the digest value and other relevant information.
- **<signaturevalue>** - It is used for storing the signature value.
- **<KeyInfo>** - It contains information about the signature certificates. For example- Public Key Certificate Information.
- **<Reference>** - It refers or points out the data that are going to be signed.
- **<DigestValue>** - The hash values calculated for the content stored, is stored in this element.
- **<DigestMehodAlgorithm>** - It is an algorithm to calculate the hash values.

A. XML Signature Format

```
<Signature ID ?>
        <SignedInfo>

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

The principal steps for XML Digital Signature are as follows:-

1) Define URI to be signed.
2) Calculate Hash value.
3) Feed value into <Reference> element with algorithm and other material.
4) Calculate hash value and signature value and standardize <SignedInfo>.
5) Feed the signature value to the <SignatureValue> element.
6) Add certificate or key information.
7) Assimilate <SignedInfo>,<Keyinfo> and <SignatureValue> element to the <Signature> element.

B. Verification of XML Digital Signature

The verification process can be converged to two cardinal steps:-

1. Confirmation of Signature – The receiver side calculates the hash values or digests values based on the received data. Further the information about the algorithm is also put into use. The result calculated is compared with the <SignatureValue> element. If a positive match is generated then it is taken that they match.
2. Validation of Reference – The calculated hash value is compared with the digest value element. If a match is obtained then it is taken that the data set hasn't changed.

If both these steps are successfully passed it is taken that the signature has passed[3].

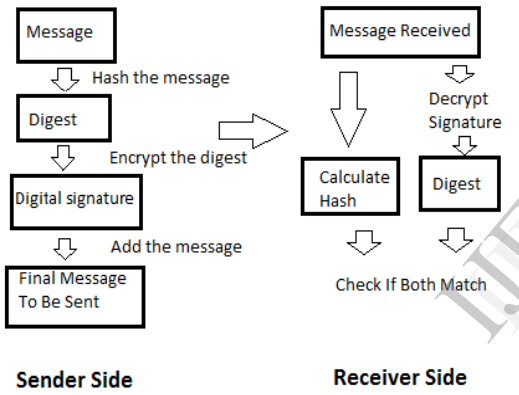

Fig.3. Digital Signature Process [5].

III. XML Encryption

XML Encryption was standardized in 2002 by W3C and is majorly implemented in XML framework of major commercial organizations such as – IBM, Microsoft etc. It is also used in various other applications such as – Health Care, Governmental and military infrastructure [6].

Shielding XML data while transferring data can be done by encrypting the message. A Slice of XML document of XML sub tree can be encrypted. These slices are encrypted with different key and hence we can distribute the same XML document to numerous users. Here each user can decrypt only some part of it [10].

A key pair is used to encrypt and decrypt data. Public key encryption of a data can only be decrypted by applying private key of the equivalent key pair. To transmit an encrypted message sender must know the receiver's public key. Every client must register their public key so that others may find their public key to transfer messages [11].

A. Encryption and Decryption Process

The encryption can also be done on other different types of data and not essentially on XML data only. XML encryption can be fundamentally explained by the following figure:

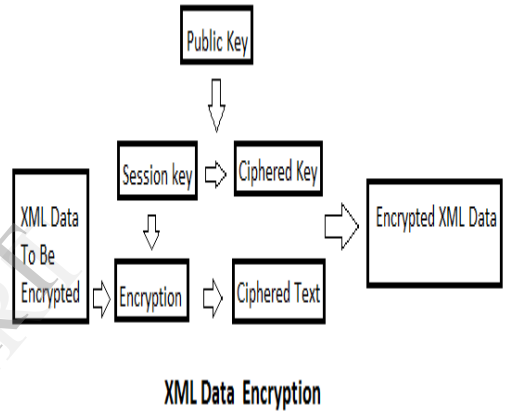

Fig.4. XML Data Encryption [4].

For Encryption:

- A random session key is generated
- The data goes through a symmetric encryption algorithm with the session key.
- The session key is encrypted with an asymmetric algorithm with the public key of the receiver.

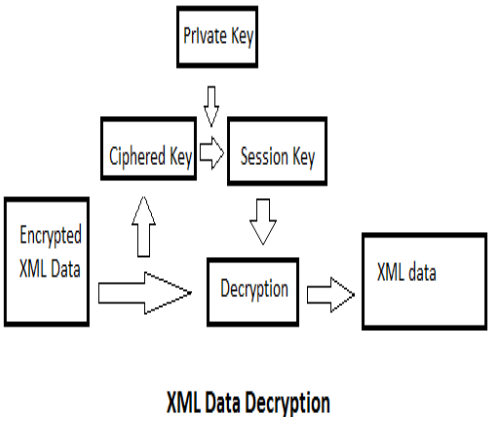

Fig.5. XML Data Decryption [4].

For Decryption:

- The encrypted session key is decrypted using a private key of the receiver. This decrypted session key was the key that was used to encrypt the data.
- The ciphered test is decrypted using the session key.

IV. XKMS (XML Key Management Specification)

The XML Key Management Specification or XKMS illustrates basic web services for exacting, authenticating and registering public keys; hence helping clients to overlook the fundamental public key infrastructure.It is divided into two primary parts. The XML Key registration service specification (XKRSS) and the key information service specification (XKISS). XKMS imparts XML-friendly validation and key management services. We now succinctly elucidate about XKRSS and XKISS. The XKRSS illustrates services relating to the registration, recoverability, reissue and revilement of keys. When a new public key is to be registered a key generation process may be performed by the client or by the service provider. If the pair is generated by the client then it is a necessity that possession of the private key be proved in order for the registration of the public key. Either ways the authentication is done by XKRSS [1]. XKRSS binds information likename, identifier etc. Generation of key may be done via client or by service on request.

If the applications composed by XML Signature are complicated, then we can reduce it by XKISS. Carrying out cryptographic verification can be problematic if data provided by the signer is scarce or it may be hard do elect whether to confide in a signature. There may also be instances where the format of signer may not be supported by the client. Communication with XKISS can be constructive to get the misplaced data. There are two service routes of XKISS: Locate and validate. Both these are employed using response/request pairs [9].

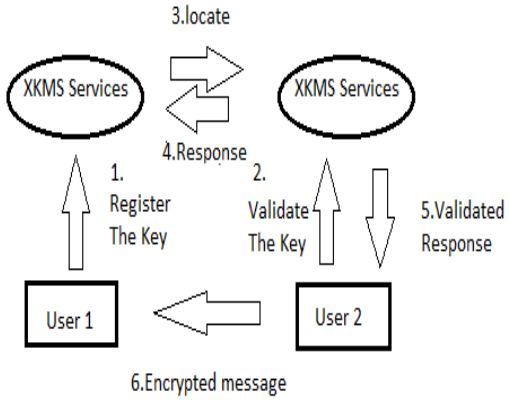

Fig.6. XKMS Services Process [1].

Let us consider the above figure. Here user2 wants to send a document which is encrypted to user1 using his public key. But user2 doesn't have user1's public key. Further even though user1 has registered his public key with XKMS service in his own domain, there is no liaison between user2 and the XKMS service present in user1's domain, hence user2 may contacts the validate service in her own domain, postulating that she requires the public key of user1 for encryption. The validation service then forwards this request to the locate service in user1's domain. This may be done through DNS. But before the response reaches user2 its validation is done by the validation service within her own domain [1].

V. Conclusion

We would like to conclude that we have successfully examined the three principal XML security components which are mainly- XML Signature, XML Encryption and XKMS (XML Key Management Specification).We have also stressed upon the fundamental basics of XML and XML Security and explained its importance. We have also by the way of illustrations explained the relevant concepts in depth.

REFERENCES:

[1] Nils AgneNordbotten, "XML and Web Services Security Standards", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 3, THIRD QUARTER 2009.

[2] Hee-Young Lim, Young-Gab Kim, Chang-Joo Moon, Doo-Kwan Baik,"Bundle Authentication and Authorization using

XML Security in the OSGi Service Platform", Proceedings of the Fourth Annual ACIS International Conference on Computer and Information Science (ICIS'05) 0-7695-2296-3/05 © 2005 IEEE.

[3] SandroGerić, TomislavVidačic, "XML Digital Signature and its Role in Information System Security", MIPRO 2012, Opatija, May 21-25,2012.

[4] Baolong Liu, Hua Chen, "Implementation a Prototype of XML Security for Certificate Management", 978-1-4577-0860-2/11, ©2011 IEEE.

[5] NargesShahgholi, MehranMohsenzadeh, Mir Ali Seyyedi, Saleh Hafez Qorani, "A new security framework against Web services' XML attacks in SOA", 978-1-4577-1127-5/11, ©2011 IEEE.

[6]TiborJager, JurajSomorovsky, "How to Break XML Encryption∗", CCS'11 October 17–21, 2011, Chicago, Illinois, USA. Copyright 2011 ACM 978-1-4503-0948-6/11/10..

[7] Tao-Ku Chang, Gwan-Hwan Hwang b, "The design and implementation of an application program interface for securing XML documents", The Journal of Systems and Software 80 (2007) 1362–1374.

[8] Onashoga, S. A. and Sodiya, A. S., "A Confidential Electronic Result Transfer Using a Hybrid XML Security Scheme", 2011 Eighth International Conference on Information Technology, 978-0-7695-4367-3/11 © 2011 IEEE.

[9] Guillermo Álvaro, Stephen Farrell, Tommy Lindberg, Roland Lockhart, Yunhao Zhang, "XKMS Working Group Interoperability Status Report", EuroPKI 2005, LNCS 3545, pp. 86-99, 2005, © springer-verlag Berlin Heidelberg 2005.

[10] Takeshi Imamura, Andy Clark, Hiroshi Maruyama, "A Stream-based Implementation of XML Encryption", Proceedings of the 2002 ACM workshop on XML security, ACM New York, NY, USA ©2002.

[11] Emerson Oliveira, ZairAbdelouahab and Denivaldo Lopes, "Security on MASs with XML Security Specifications", Proceedings of the 17th International Conference on Database and Expert Systems Applications (DEXA'06) 0-7695-2641-1/06 © 2006, IEEE.

[12] ErnestoDamiani,Sabrina De Capitanidi,PierangelaSamarati,"Towards Securing XML Web Services",ACM Workshop on XML Security, ACM 1-58113-632-3/02/0011,November 22, 2002.

[13]KayvanFarzaneh,MahmoodDoroodchi," XMLSecurity beyond XSLT",1-4244-0674-9/06 ©2006 IEEE