iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Improving Security of Network Services against WSDL Threats

Niranjan Babu .T[1], Balachandra Reddy. K[2]
[1,2]Department of CSE JNTUA College of Engineering Pulivendula

Abstract: ***WSDL documents are the guide book for attacking and hacking the web services. Since a WSDL documents contains explicit instructions on how to communicate private application, they can cause a series security breach if the web services are compromised. To the best of our knowledge, all standards which are presented by now tried to defend security problems of SOAP messages which are transferred between web services. This paper is bringing to focus enhancing security of web service's WSDL file. It purposes a model for encrypting WSDL document to handle its security problem. This solution is suitable for web services which have critical rules according their policies and their WSDL faced with hacking problems.***
Keywords: WSDL, Security, Network services, Threats

I. INTRODUCTION

Service Oriented Architecture (SOA) enables the provision of business logic as independent services. These services are loosely coupled, reusable, and can be discovered and bound on demand using appropriate service descriptions, which enables the flexibility of SOA. Most of the systems which implemented by SOA have high complexity and spread, so securing them is harder than common systems. On the other hand, distributed systems are slower than such systems in concentrate model, so security solutions for such systems should not fall down the rate.

The XML based characteristic of web service makes it available via the web no matter how different their background systems are between the service provider and service consumer. This characteristic made it as an XML based technology. In the other word, the foundation of web service technology is on XML because the main correlated components like WSDL, BPEL, and SOAP are all derivatives of XML languages. WSDL as web services interface which describes all about web service is in XML format. SOAP has a pattern of messages which are transferred between web services to make communication between service provider and service consumer also is handled as XML files. BPEL as an executable language for specifying actions within business processes with web services serialized in XML. Hence the security of web services is so involved with the security of XML. XML Signature and XML Encryption are main parts of XML security standards which have issued by World Wide Web Consortium (W3C) in 2002. SOAP secured by WS-Security which is a standard that state a strategy and specifications to bring different security technologies together. The WS-Security provides how XML Digital Signatures and XML Encryption may be used with SOAP messages.

Securing the WSDL document isn't as simple as security of SOAP messages. Requesters find the list of functions of web services and their parameter by parsing WSDL. Hackers can attack to web service by abusing this information. This contribution describes a solution to repel to hackers who want to attack to Web service by this hole. It aims to offer a security level on WSDL by using the XML security standards in order to handle this security problem.

A. Web Service Security

The suitability of web services for integrating heterogeneous system is largely facilitated through its extensive use of the XML. The interface of a Web services is far instance described using the XML based web service description language. XML based SOAP messages forms the basis for exchanging information between entities in web service systems. The information contained within these SOAP messages may be subject to both confidentiality and integrity requirement. The use of digital signatures is a common method for ensuring message integrity, authentication, and no repudiation. XML Signature defines a standard interoperable format for representing digital signatures in XML and provides mechanisms for efficiently applying digital signatures to XML resources.

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

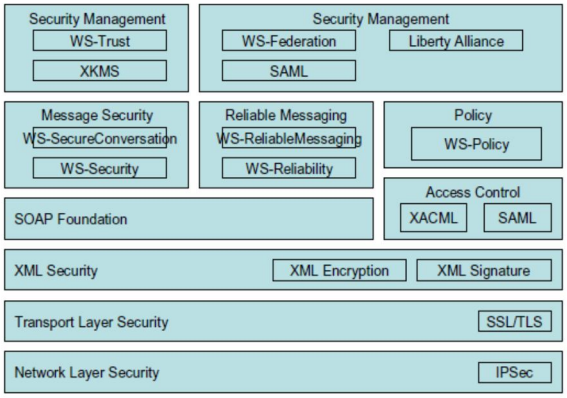


Fig 1: The web service security stack

The above figure illustrates a notional reference model for web services security standards. It maps the different standards to different functional layers of a typical web service implementation. The XML security layer in above figure provides a standard framework for XML based applications. XML Digital signature and XML Encryption are used for data confidentiality and integrity. Security Assertion Markup Language (SAML) focuses on authentication assertions. XML Access Control Markup Language (XACML) is for information access control. XML Key Management Specification (XKMS) is used to manage Public key infrastructure and web service security brings standards together. XKMS was created to be suitable for use in combination with XML Signature and XML Encryption. XKMS basically defines simple web services interfaces for key management, thereby hiding the complexity of traditional public key infrastructures from the clients.

XML Signature and XML Encryption are used to provide integrity and confidentiality respectively. Although these two standards are based on digital signatures and encryption, none of them define any new cryptographic algorithms. The use of digital signatures is a common method for ensuring message integrity, authentication, and no repudiation. XML Signature defines a standard interoperable format for representing digital signatures in XML and provides mechanisms for efficiently applying digital signatures to XML resources. Digital signature acts as a filter for recipient of a message to makes him sure that the received message hasn't been tampered and what he has received message is the exact copy of original form. XML Signature and XML Encryption may work in whole or in part of XML documents and non-XML data as well.

XML Encryption is generally using symmetric key encryption. It is also known as secret key cryptography, in which the sender and receiver use a common key for encryption and decryption. But this may cause a problem as sending confidential information to receiver, the sender and the recipient must also share the symmetric key without anyone else. This can be difficult without person to person contact. To avoid this problem and make it easier to share confidential contents with a number of people, asymmetric or public key cryptography was designed. Public key cryptography uses a matched pair of keys, one for encryption and for decryption. In this encrypt process, the sender encrypts using the recipient's public key that can be shared widely. The recipient decrypts using private key that known only to them. The symmetric key is used to encrypt the content, and then the symmetric key is encrypted using public key cryptography.

In comparison symmetric encryption is faster than asymmetric encryption, but it needs a secure channel for transferring the shared secret key, whereas asymmetric pattern doesn't need this channel because of using two different keys for encrypting and decrypting messages. WS-security specifies how to apply XML security standards to SOAP messages.

B. WSDL Attacks

In order to illustrate the nature of the WSDL threats, it is necessary to discussing about the structure of WSDL documents.

II. A BRIEF OVERVIEW OF WSDL

In SOA, WSDL is used to describe the interfaces of all services irrespective of the underlying technology. It describes the web services and WSDL 2.0 has simplified the interface description. The interface is defined within the <interface> section. It has dropped the concept of input and output messages. It has introduced the message exchange patterns, which specify the sequence in which the associated messages are to be transmitted between the service and the client. It is also allows interface inheritance.

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A. WSDL Threats

WSDL documents are the handbook to a company's web services, and as such, they contain the recipe for interaction that yields improved communication between organizations. WSDL documents are also the handbook for attacking and hacking these same web services. The two important threats of WSDL documents are "WSDL Scanning" and "Parameter tampering" in WSDL scanning threat, attackers may reveal sensitive information like types, messages, operations port types, bindings, and guess other methods. In parameter tampering, attackers tamper parameters within WSDL document in order to retrieve unauthorized information. Since structures on how to use parameters are explicitly described within a WSDL document, malicious users can play around with different parameters to access confidential information.

III. ENHANCING SECURITY OF WSDL

WSDL file determines all functionality attribute of web service. Everybody can access WSDL to find needed information for call an operation of web service. Therefore it acts as a guidebook for hackers to use it and halt a web service. Enhancing security of WSDL is provided by applying a security level on WSDL documents to protect it against malicious access. A requester who wants to use WSDL should follow a scenario up in order to obtain needed information, so the access time increased. The proposed approach is adoptable with WSDL versioning to apply change management.

Our approach is illustrated in below figure. It tries to show the steps of applying the security level on WSDL document. The components which show in this figure are given below.

A. "Web Service Provider" which presents a set of services for customers.

B. UDDI which is specification for defining a registry of information for discovery of Web services. It provides a feature to publish and discover information about Web services.

C. "Encryptor" Service is a Web service which is defined as a main component of our approach in order to encrypt WSDL document.

D. "Key Generator service" is another part of this approach that generates and manages keys which are needed in encryption algorithms.

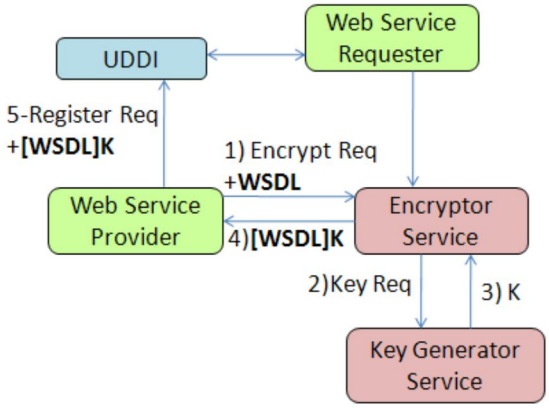


Fig 2: Enhance the security of WSDL document

The steps of this approach as in the figure are:

Step1: Web service provider sends a request to Encryptor Web service to ask him to encrypt the original WSDL document.

Step2: Encryptor gets the request. He should encrypt received WSDL via XML Encryption protocol. Either symmetric or asymmetric encryption needs a key for applying algorithm. So he sends a request to Key Generator service.

Step3: Key Generator produces keys and response the received request.

Step4: Encryptor encrypts the WSDL document and sends it to provider. He can use symmetric or asymmetric algorithm. Selecting the best one is depending on the environment. If a secure channel is available, then symmetric encryption can be used and shared a key be transferred via this channel and Encryptor doesn't need to know who the requester of web service is. On the other hand, in asymmetric encryption the public key of users should be saved and managed in a key management infrastructure which is so expensive.

Step5: Provider registers his service in UDDI and submits encrypted WSDL as his description file in registry. Now encrypted WSDL is accessible for everyone.

E. A Short Summary of Approach's Steps is

1) Provider --------> Encryptor: Encrypting request, original WSDL
2) Encryptor --------> KeyGenerator: Key Request
3) Key Generator ---------> Encryptor : K
4) Encryptor ---------> Provider: [WSDL] K
5) Provider ---------> UDDI: Registering [WSDL] K request

By following these steps a security level applied on WSDL and hackers can't access to it. All users face to an unmeaning WSDL document and can't gain ant information from it, unless they decrypt it.

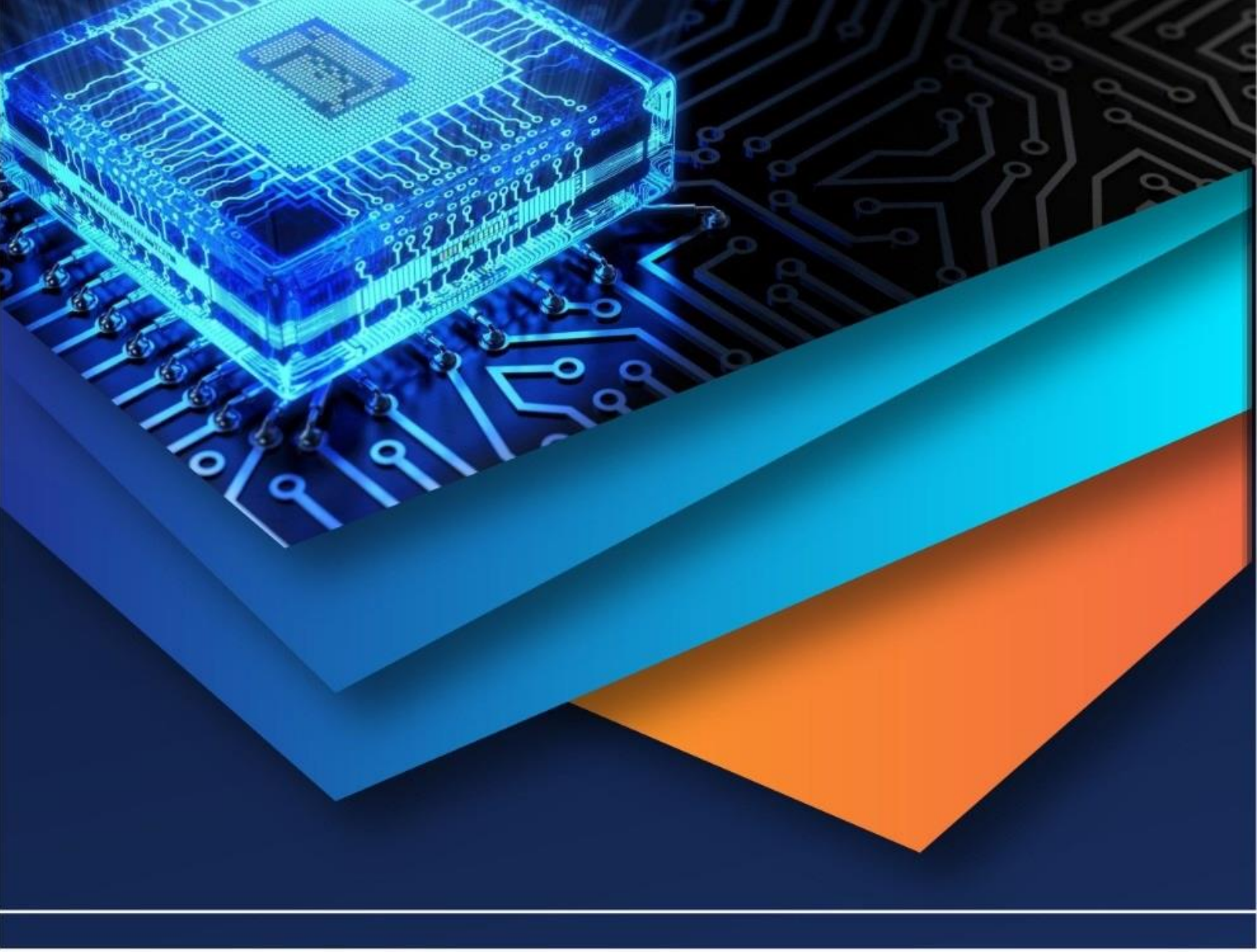
Service requester should decrypt this file to gain needed information, so he needs the respective key to decrypt it. If the symmetric encryption has been applied, the requester will use his own private key to decrypt the document, else if the symmetric encryption has been used, then the requester should use shared key for decrypting. He can obtain it via a secure channel to encryptor. Notice that he can't obtain the key unless he authenticated to Encrypt service. There are lots of authentication algorithms which can be used like Kerberos.

IV. CONCLUSION

Security of WSDL is a challenging area in Web service security which doesn't discuss in previous standards. Web service security architecture brings different security technologies together and offers a new standard as WS-Security which focuses on security of SOAP. The WS-Security specification provides how XML Digital Signatures and XML Encryption may be used into SOAP messages. This paper presents a solution to secure WSDL document. A brief introduction to XML and Web services security standards and how they work together had been proposed. The solution for providing the security of web services against WSDL threats had been proposed.

REFERENCES

[1] S.Gaitherburg,"Web Services Security: Challenges and Techniques", IEEE International Workshop on policies for Distributed Systems and Networks, vol.7, pp.282-288, June 2007.
[2] Robert Warschofsky, Michael Menzel, and C. Meinel, "Transformation and Aggregation of web service security requirements", IEEE Computer Society, pp.43-50, 2010.
[3] P Lindstorm,"Attacking and defending web services", Spire Security Research Report January 2003.
[4] Web Services Description Language (WSDL) Version 2.0:W3C, 2007.
[5] Web Services Description Language (WSDL) 1.1:W3C, 2001.
[6] N.A.Nordbotten,"XML and Web Services Security Standards", IEEE Communication Survey & Tutorials, Vol. 11,pp.4-21, 2009.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY