IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. V (May – Jun. 2015), PP 35-39
www.iosrjournals.org

Algorithm for Securing SOAP Based Web Services from WSDL Scanning Attacks

Mohamed Ibrahim B[1], Mohamed Shanavas A R[2]
[1]*Software Solution Architect & Research Scholar*
[2]*Associate Professor, Jamal Mohamed College, Tiruchirappalli, India*

Abstract: *The Web Services are the emerging paradigm of Service Oriented Architecture (SOA) in the modern enterprise computing to achieve interconnection of related applications in an organization in terms of services. A service is a Software component which fulfills a defined functionality and does not depend on the context of other services. In programming terms, the service is called as web method which is a function that accepts input parameters and returns the output. The data types of input/output parameters may be simple or complex. In SOA architecture, the list of web methods that a web service offers and the data types of their input/output parameters are described using Web Services Description Language (WSDL) standard and published to Universal Description, Discovery and Integration (UDDI) service registry where the web services clients search the service registry for obtaining the required WSDL and start binding to the web server. The WSDL is prone for SOA attacks as the WSDL is represented in XML format which is a plain text. Even though few researchers proposed solutions for WSDL, those solutions are inadequate concerning to the modern communication technologies and they are not able to achieve any landmark in providing security for WSDL attacks. This paper proposes a new algorithm for preventing WSDL attacks which uses the existing security standards such as Public Key Infrastructure (PKI), Digital Signatures, and XML Encryption/Decryption standards.*

Keywords - *SOA, Web Services, Security, WSDL, PKI, Computer Networks*

I. Introduction

In order to integrate the related applications in an enterprise, several standards such as RMI, CORBA and DCOM are used earlier. These standards adhere to the Service Oriented Architecture (SOA) where a service is a component in an application which fulfills the defined functionality where it does not depend on the context of other services. However, these standards belong to specific vendors and depend on the languages, platforms and machine architectures. The Web Services are the emerging model in SOA which uses standard Internet protocols for communication between web server and its clients. The Internet protocols are supported by majority of machine architectures and platforms and the web services use simple XML format for data exchange. As all the modern programming languages are comfortable to parsing XML formats, web services can be developed and maintained in any language, thus provides language independent.

The list of available services, their input/output parameters and data types are described using Web Services Description Language (WSDL). The WSDL is a standard recommended by World Wide Web Consortium (W3C). The latest version of WSDL is 2.0 [1] and its previous standard version is 1.2 [2], where the structures of both versions are different. The web service descriptions are published in Service Registry using Universal Description, Discovery and Integration (UDDI) standard where the web service clients will look into this registry for the required service description and start communicating with service provider. Thus the standard SOA architecture contains three important components: (i) Service Provider, (ii) Service Registry and (iii) Client. The three different basic operations that can be performed in SOA architecture are: (i) Publish by Service Provider to Service Registry, (ii) Find by Client from Service Registry and (iii) Bind by Client to Service Provider [3].

In this paper, we concentrate on providing security for "publish" and "find" part of SOA architecture, i.e. protecting WSDL operations in order to prevent attackers to attack web services by gaining advantage of interpreting WSDL content which is in plain text format.

This paper is organized as: Section 2 reviews the available literature for WSDL attack prevention, the proposed algorithm for protecting SOAP web services from WSDL attacks is explained along with proof-of-concept and result analysis in Section 3, and Section 4 concludes the paper.

II. Literature Review

Reviewing literature, we can see many researchers shown interest in protecting message level attacks, which may occur during web service request and response between web service client and web service provider. Only very less researchers are provided solutions for WSDL attacks. In fact, the WSDL attacks are severe which

may halt the entire web services down and provides opportunity for attackers to retrieve sensitive information of the organization.

Mirtalebi et al. [4, 5] and Narges et al. [6, 7] proposed security solutions in the form of framework for defending WSDL attacks. Both the researchers use the symmetric key cryptography for securing the WSDL content before publishing it to service registry. However the key maintenance methods and key exchange mechanisms in order to receive the symmetric from the service provider are not clearly defined in their papers.

The security solutions that are provided by vendors only work as part of their products and they have few implementation constraints. At present, there is no comprehensive security solution defined for preventing WSDL attacks.

III. Proposed Algorithm for Preventing WSDL attacks

The proposed algorithm uses the XML encryption standard to protect the WSDL scanning attacks on the SOAP based web services. It does not aim to encrypt the entire WSDL which is represented XML format, but only the critical portion through which the attacks can interpret the important information of the defined services such as the exposed service names along with their input/output parameters.

The custom security elements are added with WSDL segment in order to notify the clients the retrieved WSDL from the service registry is encrypted and the clients are needed to descript before they bind to the web server. The security algorithm use symmetric key cryptography for encrypting the content of the WSDL and asymmetric key cryptography for validating service provider/service requester of web service. The hashing algorithm such as MD5/SH-1 is applied to ensure the message integrity of the WSDL content transmission.

It is assumed that the service provider and requester trust on the same Certificate Authority (CA) in order to create and validate digital signatures. To maintain the digital certificates, the existing PKI and XMKS standards are used.

The proposed algorithm uses the existing security standards as stated below.

- Symmetric Key Cryptography for encrypting the WSDL content at Service Provider [8].
- Hashing Algorithm for generating digest for ensuring message integrity to check whether the received message at the web service client is not altered by the intermediate nodes passed through from service registry.
- Public Key Infrastructure (PKI) and XML Key Management System (XKMS) are used for maintaining private/public keys of using asymmetric key cryptography. Private Key is used for encryption and Public Key is used for decryption, and vice versa [9, 10]
- Digital Signatures for ensuring the request/response is from right resource [11].
- Certificate Authority (CA) for maintaining digital certificates used for digital signatures.
- A new Software component named "Intelligent Security Engine (ISE)" is introduced at Service Provider end which is the implementation of the proposed security algorithm at server side.
- The ISE can be placed in a proxy server so that it can serve for many web servers in which different web services are running. Even it can be attached to Enterprise Service Bus (ESB) network, through which security can be applied to the entire Enterprise Application Integration (EAI) components.

The proposed security algorithm for protecting SOAP web services from WSDL attacks are given in Figure 1 and Figure 2 respectively for service provider and service requester side. The flow chart representation of the proposed algorithm is outlined in Figure 3.

As proof-of-concept (POC), the proposed algorithm is implemented using Java technologies and tested in web service environment with real time banking data. From the preliminary analysis of the result, we can see that the extra time taken by web services after the implementation of this security concept is minimal and acceptable.

Algorithm: WSDL_Attack_Prevention_At_Server_Side

Input: WSDL file
Variable: wsdl: WSDL file;
PriKSP: Private Key of Service Provider;
DSignSP: Digital Sign of SP; Digest: Hash of WSDL content;
SymK: Symmetric key; encWSDL: Encrypted WSDL file
Output: Encrypted WSDL

Begin

Step I: /* Service Provider sends WSDL to ISE */
wsdl = WSDL(SP)

Step II: /* Generates values for Keys and Hash; Assign to variables */
Call XKMS, KeyGen, Hash modules

Step III: /* Encrypt WSDL */
encWSDL = $[wsdl + [Digest]_{PriKSP} + DSignSP]_{SymK}$ + Custom_Security_Elements

Step IV: /* Publish encWSDL */
Call UDDI Directory Service API
Service Registry ← encWSDL

End

Figure 1: WSDL Attack Prevention (at Server Side)

Algorithm: WSDL_Attack_Prevention_At_Client_Side

Input: Encrypted WSDL file
Variable: wsdl: WSDL file; digest: Hash; SymK: Symmetric key; encWSDL: Encrypted WSDL file
Output: WSDL

Begin

Step I: /* Service Requester gets WSDL from Service Registry*/
Call UDDI Directory Service API;
Service Requester ← ServiceRegistry[WSDL]

Step II: /* Check whether received WSDL is encrypted */
If Custom_Security_Elements found Then
encWSDL = Received WSDL
Else
Display "WSDL is not encrypted";
End If

Step III: /* Get Symmetric Key from Service Provider using PKI and Decrypt WSDL */
wsdl = $[encWSDL]_{SymK}$

Step IV: /* Calculate Digest of the decrypted WSDL & Compare it against received Digest */
If Calculated_Digest = Received_Digest Then
WSDL is not altered; Initiate binding process with Service Provider
Else
WSDL content is altered; Report to ISE;
End If

End

Figure 2: WSDL Attack Prevention (at Client Side)

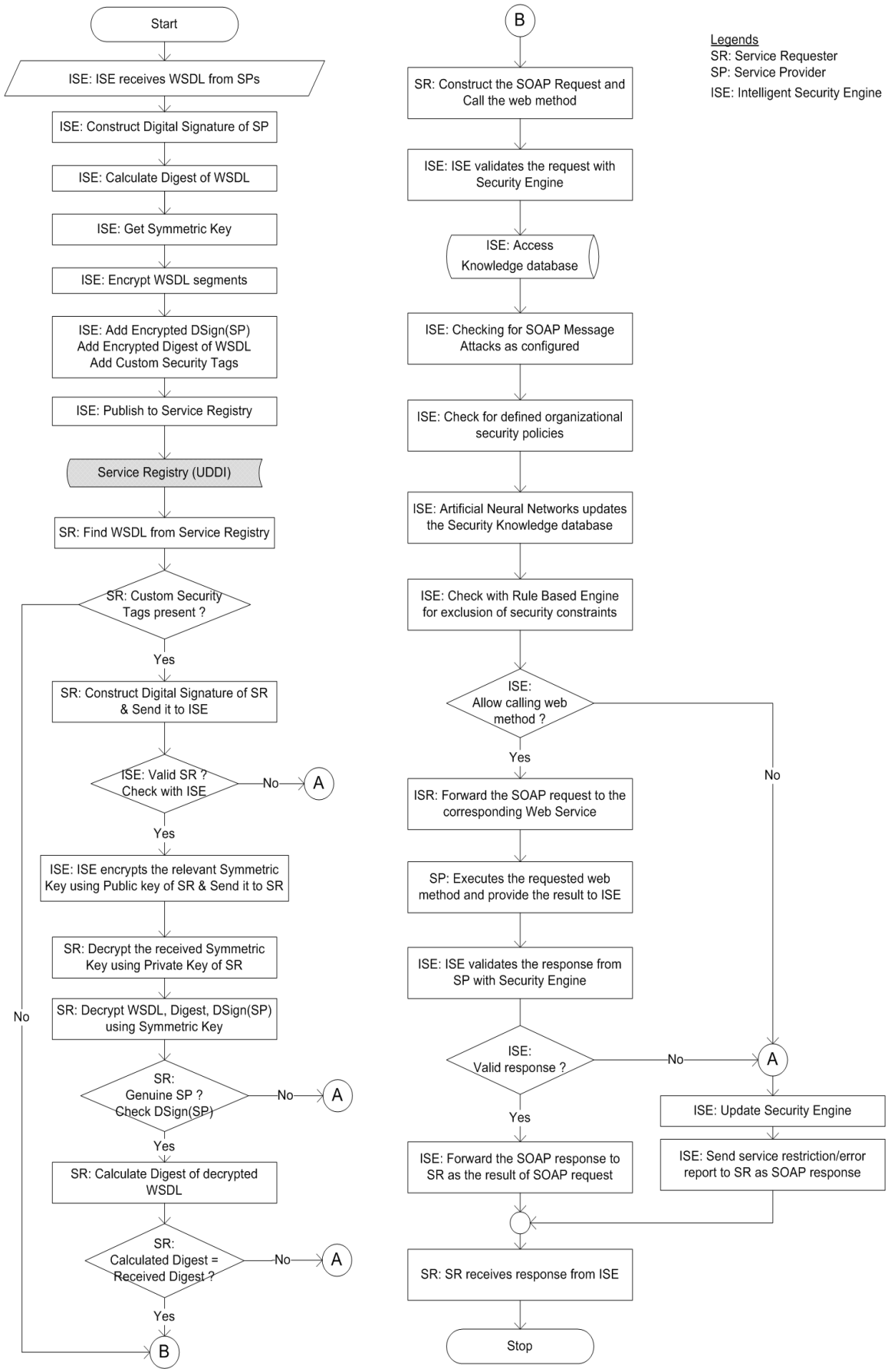

Figure 3: Flow chart representation of the proposed security algorithm

IV. Conclusion

The earlier technologies for SOA such as RMI and CORBA are already sunset by the industry, and the web services are preferred choice of enterprises for the implementation of SOA. The web services use XML as data exchange format for its communication with service provider, service registry and service requester. As the XML format is in a simple text, it is prone for attacks. From scanning the WSDL, an attacker can become to know the list of available services along with their input/output parameters and their data types. It became vulnerability for web service where the attackers can use these retrieved information in order to make attacks on SOAP web services. A new security algorithm is proposed in this paper to protect the web services from the WSDL attacks. As a novelty, this algorithm uses a specialized security component named "Intelligent Security Engine" which can be configured to identify any kind of WSDL attacks. The proposed algorithm is implemented and tested with real time data and results are as expected in terms of performance.

References

[1]. WSDL 2.0 Specifications: http://www.w3.org/TR/wsdl20/
[2]. WSDL 1.2 Specification: http://www.w3.org/TR/wsdl
[3]. Danish Jamil and Hassan Zaki, "Security Implication of SOAP and Web-Service Interface to the Cloud Computing System," International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462 Vol. 3 No. 4, 2011
[4]. Mirtalebi, Arezoo, and Mohammad Reza Khayyambashi, "Enhancing Security of Web Service against WSDL Threats," 2nd IEEE International Conference on Emergency Management and Management Sciences (ICEMMS), pp. 920-923, IEEE, 2011.
[5]. Mirtalebi, Arezoo, and Mohammad Reza Khayyambashi, "A new Security Framework for Protecting WSDL File of Web Service," Internatinal Journal of Computer Science and Network Security (IJCSNS), Vol. 12, No. 9 , pp. 84-90, 2012.
[6]. Shahgholi, Narges, Mehran Mohsenzadeh, Mir Ali Seyyedi, and Saleh Hafez Qorani, "A New SOA Security Framework Defending Web Services Against WSDL Attacks," IEEE 3rd Inernational Conference on Privacy, Security, Risk and Trust (PASSAT), pp. 1259-1262, IEEE, 2011.
[7]. Shahgholi, Narges, Mehran Mohsenzadeh, Mir Ali Seyyedi, and Saleh Hafez Qorani, "A New Security Framework against Web Services' XML attacks in SOA," The 7th International Conference on Next Generation Web Services Practices, pp. 314-319, IEEE, 2011.
[8]. Singh Preeti, and Praveen Shende, "Symmetric Key Cryptography: Current Trends," International Journal of Computer Science and Mobile Computing, Vol. 3, Issue 12, pp. 410-415, 2014.
[9]. Chan, Dan TF, and Lucas CK Hui, "Towards a unified PKI Framework," International Symposium on Technology Management and Emerging Technologies (ISTMET), pp. 113-118. IEEE, 2014.
[10]. XML Key Management Specification: http://www.w3.org/TR/xkms2/
[11]. Cash, David, Rafael Dowsley, and Eike Kiltz, "Digital Signatures from Strong RSA without Prime Generation," Public-Key Cryptography (PKC 2015), pp. 217-235, Springer Berlin Heidelberg, 2015.