# Research on the Model of Secure (System Security) Transmission of SOAP Messages

Samir Nepal, Surbhi jaiswal, Sonu kumar, Ashish kumar, (Guidance) HOD of ADESH C.K Raina
*Adesh group of institution, Gharuan mohali*

**Abstract-** SOAP as the basis application of Web Services, and, SOAP messages are closely related to the heterogeneous Web services. Secure transmission of SOAP messages play a vital role for the applicability of Web Services. The main challenges to the secure transmission of SOAP messages includes: confidentiality, authentication, integrity, both-party nonrepudiation, and single sign-on. SOAP, the Simple Object Access Protocol, is a protocol that allows the exchange of structured data between peers in a decentralized, distributed environment. The structure of the data being exchanged is specified by an XML scheme.The fact that SOAP messages are encoded in XML makes SOAP messages portable, because XML is a portable, system-independent way of representing data. By representing data using XML, you can access data from legacy systems as well as share your data with other enterprises. The data integration offered by XML also makes this technology a natural for Web-based computing such as Web services. Firewalls can recognize SOAP packets based on their content type (text/xml-SOAP) and can filter messages based on information exposed in the SOAP message header.

The SOAP specification describes a set of conventions for exchanging XML messages. As such, it forms a natural foundation for Web services that also need to exchange information encoded in XML. Although any two partners could define their own protocol for carrying on this exchange, having a standard such as SOAP allows developers to build the generic pieces that support this exchange. These pieces might be software that adds functionality to the basic SOAP exchange, or might be tools that administer SOAP messaging, or might even comprise parts of an operating system that supports SOAP processing. Once this support is put in place, other developers can focus on creating the Web services themselves.

***Keywords:*** SOAP messages, Web Services, secure transmission model, both-party nonrepudiation, single signon., Audit log-System Access, 2-factorAithentication.

## I. INTRODUCTION

Soap is a simple solution for interaction of different applications built in different languages and running on [1] different platforms as it uses HTTP as its transport and XML as its payload for sending and receiving messages. Its is a lightweight and a loosely coupled protocol for exchange of information in a decentralized and a distributed environment. Web Services are already a reality for many organizations and are just around the corner for most of the rest of us. One of the core specifications on which Web Services rely heavily is SOAP (Simple Object Access Protocol). In terms of a services-oriented architecture, SOAP is used to send data from one application to another. Most proprietary protocols require the applications of the same breed to be running on both the ends, what if the server is implemented in a different programming language. The ability to access service of a component in a language/location and platform transparent manner reduces the tight coupling between the client and the server. SOAP enables "incompatible" systems to interoperate. [2].

```
<SOAP:Envelopxmlns:SOAP="urn:schemas-xmlsoap-org-
soap.v1">
<SOAP:Header></Soap:Header>
<SOAP:Body>
<Add>
<Num1>100</Num1>
<Num2>400</Num2>
</Add>
<SOAP:Body>
</SOAP:Envelop>[2]
```

One of the goals of SOAP designing is simplicity, so security was not taken into account by the SOAP specification. SOAP messaging security relies on the established security concepts and technologies, such as , encryption, digital signature, authentication, and data integrity. This paper is to study the secure transmission of SOAP messages.

## II. RELATED WORK

SOAP, which is a messaging protocol based on XML, is about sending messages, meaning that it specifies a way to send XML-based messages from one process to another, usually from one machine to another. More specifically, SOAP is a protocol that specifies an enveloping mechanism for sending data (via XML). Furthermore, it specifies how to send these messages to a final destination, and the processing model that applies if that message goes through several intermediaries. And, it specifies how to do this over HTTP.

The SOAP specification describes four major components: formatting conventions for encapsulating data and routing directions in the form of an envelope, a transport or protocol binding, encoding rules, and an RPC mechanism. The envelope defines a convention for describing the contents of a message, which in turn has implications on how it gets processed. A protocol binding provides a generic mechanism for sending a SOAP envelope via a lowerlevel protocol such as HTTP. Encoding rules provide a convention for mapping various application datatypes into an XML tag-based representation. Finally, the RPC mechanism provides a way to represent remote procedure calls and their return values. As to the structure, a SOAP message consists of an envelope containing an optional header and a required body, as shown in Figure 1. Envelope, the topmost container, comprises the SOAP message; Header contains additional blocks of information about how the body payload is to be processed; and Body contains the actual message to be processed. Each element contained by the Header is called a header block. The purpose of a header block is to communicate contextual information relevant to how the message is to be processed. This includes routing and delivery settings, authentication or authorization assertions, and transaction contexts. XML elements and attributes for the purpose of SOAP security are just placed inside the SOAP header. The body contains the actual message to be delivered and processed. Anything that can be expressed in XML syntax can go in the body of a message.

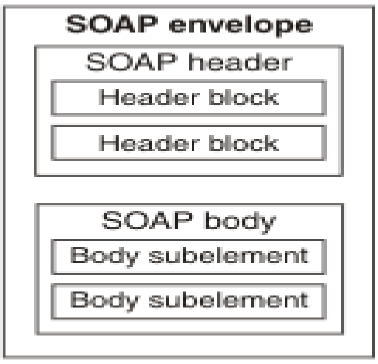

Fig.1: SOAP message structure.

A SOAP message can be anything: a purchase order, a request for a current stock price, a query for a search engine, a listing of available flights, or any number of other pieces of information that may be relevant to a particular application. .While a SOAP message is fundamentally a one-way transmission of an envelope from a sender to a receiver, that message may pass through various intermediate processors that each in turn do something with the message. The set of intermediaries that the message travels through is called the message path. Every intermediary along that path is known as an actor. SOAP dose specify a mechanism of identifying which parts of the SOAP message are intended for processing by specific actors in its message path. This mechanism is known as “targeting”. Targeting can only be used in relation to header blocks, and the body of the SOAP envelope cannot be explicitly targeted at a particular node. The value of the actor attribute is the unique identifier of the intermediary being targeted. Intermediaries that do not match the actor attribute must ignore the header block[3]. The construction of a message path (the definition of which nodes a message passes through) is not covered by the SOAP specification. Various extensions to SOAP, such as Microsoft's SOAP Routing Protocol (WS-Routing) have emerged to fill that gap. WSRouting defines a standard SOAP header block for expressing routing information. Its role is to define the exact sequence of intermediaries through which a message is to pass.

## Proposed Model of Secure (Security services)Transmission of SOAP Messages

In an enterprise application scenario, along with the involvement of purchase order, services providing, and payment, the information integration among enterprises extends security boundary from intranet to internet. Naturally, the risk of security increases evidently.

SecurityAnalysis of SOAP messages transmission

The division of information security into logical components makes it easier to understand, and therefore easier to deploy[2]. These logical components, each of which maps a challenge to the security of SOAP messages transmission, are confidentiality, authentication, integrity, and nonrepudiation.

*Confidentiality* refers to protecting information from being accessed by unauthorized parties. In other words, only the people who are authorized to do so can gain access to sensitive data. Imagine your bank records. You should be able to access them, of course, and employees at the bank who are helping you with a transaction should be able to access them, but no one else should. A failure to maintain confidentiality means that someone who shouldn't have access has managed to get it, through intentional behavior or by accident. Such a failure of confidentiality, commonly known as a *breach*, typically cannot be remedied. Once the secret has been revealed, there's no way to un-reveal it. If your bank records are posted on a public website, everyone can know your bank account number, balance, etc., and that information can't be erased from their minds, papers, computers, and other places. Nearly all the major security incidents reported in the media today involve major losses of confidentiality.

Authentication is an identity-authenticating process. In the web services world, answering the following questions is vitally important:

Who am I?

How do I prove who I am?

Why should you trust me when I tell you who I am?

Who are you?

How can I prove that you are who you say you are?

Why should I trust you when you tell me who you are?

Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

Users are usually identified with a user ID, and authentication is accomplished when the user provides a credential, for example a password, that matches with that user ID. Most users are most familiar with using a password, which, as a piece of information that should be known only to the user, is called a knowledge authentication factor. Other authentication factors, and how they are used for two-factor or mutifact

Integrity has a special meaning in the field of information security. It does not mean that information cannot be tampered with. It means that if information is tampered with, this tampering can be detected. In an untrusted network, it may be impossible to ensure that the data is tamper-proof when it is in transit to its destination. So, knowledge about the fact that tampering has occurred is the next best thing.

Nonrepudiation literally means that the originator of a message cannot claim not to have sent a given message. Nonrepudiation, which promises that malicious message sender cannot deny the fact he has sent the message, and so promises that the constructor and sender of the message is same, is vitally important to B2B and C2C(coporater to corporater) applications. Furthermore, the nonrepudiation is a both-party concept in the messaging in B2B applications. Besides the attacks launched by the sender and the malicious third-party, malicious receiver attack is to be protected to fulfil both-party nonrepudiation.

a. Technologies and Solutions that Address the Security of SOAP Messages Transmission

SOAP does not yet have a standard binding for reliable messaging. The security provided by HTTPS cannot satisfy the more and more complicated requirement of SOAP message security. A number of technologies ansolutions have been developed for the security of SOAP message transit. Several vendors offer reliable messaging solutions[4].

XML Encryption provides not only a way of encrypting portions of XML documents, but also a means of encrypting any data and rendering the encrypted data in XML format. XML Encryption is ideal for confidentiality. The ability to selectively encrypt XML data makes XML Encryption very useful for Web Services. By selectively encrypting data in the SOAP message, certain information may be hidden from SOAP intermediaries as it travels from the originator to the destination Web Services.

XML Signature explains how to express the digital signature of any data as XML, as well as explaining how to digitally sign portions of an XML document. The power of XML Signature for Web Services is the ability to selectively sign XML data. For example, if a single SOAP parameter needs to be signed but the SOAP message's header needs to be changed during routing, an XML Signature can be used that only signs the parameter in question and excludes other parts of the SOAP message. If the SOAP request passes through intermediaries route to the destination Web Service, XML Signature ensures end-to-end integrity.

Security Assertions Markup Language (SAML) provides a means of expressing information about authentication and authorization, as well as attributes of an end user in XML format. SAML does not provide authentication, but can express information about an authentication event that has occurred in the past. By authenticating once, being authorized, and effectively reusing that authorization for subsequent Web Services, single sign-on for Web Services can be achieved. If an entity is authorized based on the fact that they were previously authorized by another system, this is called "portable trust[2]".

The XML Key Management specification (XKMS) enables PKI services such as trustworthily registering, locating, and validating keys through XML-encoded messages. PKI is a system that allows public keys to be trusted by providing key signing and key validation services. Although accepted as an important, even vital, technology, PKI has a reputation for being notoriously difficult to implement. By leveraging the benefits of XML and by learning from past experiences with preXML PKI architectures, XKMS makes PKI practical for common use.

Microsoft's Passport technology takes a different approach to single sign-on. The user authenticates to the passport infrastructure, either directly through www.passport.com or through an affiliate site that makes use of functionality provided by passport.com. Once the user is authenticated and authorized by Passport, their authentication status is also available to other Web Services that use Passport[2].

Another industry proposal for the single sign-on on the Web is the Liberty Alliance Project, championed by Sun. The Liberty Alliance Project aims to enable a noncentralized approach to single sign-on, termed a "federated network identity." It appears the Passport proposal by Microsoft may be taking a similar tack to the Liberty Alliance Project[2].

WS-Security, which has emerged as the de facto method of inserting security data into SOAP messages, is primarily for securing SOAP messages. WS-Security explains how technologies such as XML Signature, XML Encryption, and SAML are used for Web Services security in particular. WS-Security defines placeholders in the SOAP header in order to insert security data, how to add encryption and digital signatures to SOAP messages, how security tokens are contained in SOAP messages, and how XML Security specifications are used to encrypt and sign these tokens. In practice, this means defining the XML elements and attributes that are used to enclose tokens into SOAP messages, and the means to enclose XML Signature and XML Encryption into SOAP[5].

b. The Architecture and Mechanism of the Secure Transmission Model

A model of secure transmission of SOAP message is developed here to fulfill the security requirement. The building blocks of the model includes: confidentiality, authentication, integrity, both-party nonrepudiation, and single sign-on. Security of the model is achieved through inserting security blocks into SOAP header, as well as adopting technologies such as XML Encryption and XML Signature. Figure 2 is the architecture of the model.

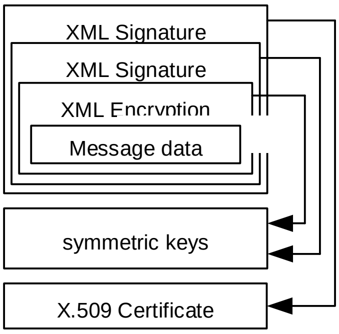

Fig.2: Architecture of the model

The arrowed lines in Figure 2 represent the reference to the keys or token.

The basic idea is: encrypting the body data using the symmetric keys, signing the encrypted data using the symmetric keys again, and then signing again the signed data, making use of the private key provided by the X.509 certificate of the recipient.

Firstly, XML Encryption is implemented upon the message data, to realize the confidentiality of message data. The result of the encryption to a resource forms EncryptedData, which will replace the original resource being encrypted. How many resources are there to be encrypted, as many EncryptedDatas will be generated. Here, encryption to message data adopts symmetric keys, which are produced randomly every time.

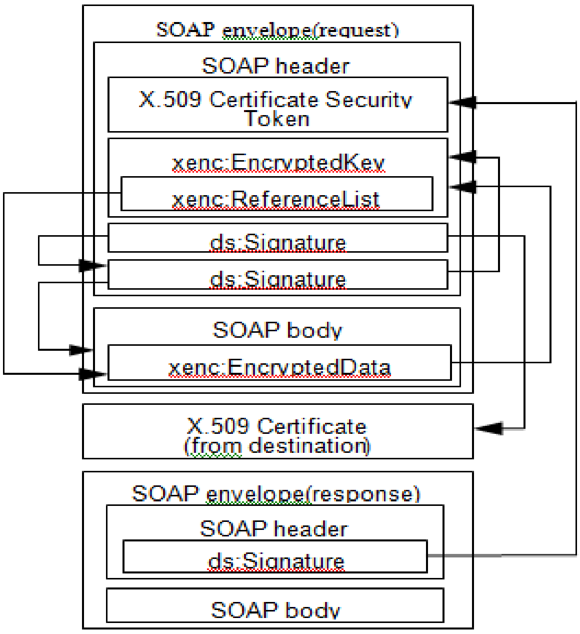

fig.3: Mechanism of the model

After being received, the second XML Signature is decrypted and verified. If the integrity is available, the keys, signature method, digest method, and encryption key can be obtained credibly. Thus, the original SOAP information is securely transmitted from the sender to the recipient. The client X.509 certificate and server X.509 certificate supply the asymmetric keys which are necessary in secure transit of the symmetric keys used in XML Encryption and XML Signature.

Figure 3 shows how the security mechanism of the model is established. In Figure 3, the arrowed solid lines represent the reference to the keys or token, well the arrowed dashed lines represent the secure operation.

### III. Security Analysis of the Secure Transmission Model

XML Encryption to the SOAP message body realizes the confidentiality of the data, and XML Signature to the encrypted data realizes the integrity of the data. Evidently, the encrypting(decrypting) speed of symmetric keys is much faster than the encrypting(decrypting) speed of asymmetric ones. The practice that the symmetric keys used in XML Encryption and XML Signature are produced randomly is securer than the symmetric keys produced using hashing method, because as for the latter, once the keys were captured, succedent transmission would lose security. Through introducing the both-party X.509 certificate (those of client and server), which contain both the asymmetric keys and the identity information of the entity, the preceding security transmission model of SOAP messages acquires a high-level transmission security, as well as enjoys the benefit of high efficiency. The solution to single sign-on is to include information about the end user in the SOAP message itself. Furthermore, by making use of the identity information of the entity, the transmission mechanism realizes bothparty nonrepudiation and single sign-on. The model itself is simple and light, but its running requires the support of certificate release of requester and responser. That is, the main load of the whole work is borne by certificate infrastructure. This maybe represents the shortcoming of it.

## IV. CONCLUSION AND EXPECTATION

Now in present world there is many problem about the hacking of the data for many porpose .so that loss of data increase . due to which directly lead to loss of money.for the security to encrypted the sending message we should make more powerfull so that instead of taking the random number from the our data base ,we can change this massage in different language ,it mean that ,if persone try to send the massage from asian to Europe the our data be change to African language within randomly .by taking location of the sender and receiver we can use different from both.so soap massage passing is more powerful then now.

Now about the login setting and massage passing ,we can use one devices which will contain the both decrypted as well as anti decrypted data ,if unknow persone try to log then its send the antiencrypted data and lead to be out of services .if know persone is try to log then its follow the decrypted data . so it also make our soap massage passing is more powerful

Aiming at the challenges that SOAP messages transmission faces in Web Services applications among enterprises, a simple and light transmission model is developed, based on existing technologies. Analysis indicates that the model fulfils the security requirement of SOAP messages transmission: confidentiality, authentication, integrity, both-party nonrepudiation, and single sign-on, enjoying well advantage and efficiency. The cost of this kind of advantage and efficiency is the deployment of X.509 digital certificate on applications communicating via SOAP messages.

It is important to keep the entire security context of the Web Service in mind. This includes properly configured firewalls, the use of patched and lockeddown Web servers, and (especially if digital certificates are used) the use of an adequate security policy document. It would be foolish to address just the new security challenges posed by Web Services and leave a system open to attack through more traditional channels.

There is a lot of work to do to strive for higher security of SOAP messages transmission, or even Web Services. To heighten the security and efficiency of the model, a particular block can be inserted into the SOAP header. Add a mustUnderstand="true" attribute to the header block, and require that the recipient must understand it. If this flag is present, and the recipient does not understand the block to which it is attached, the recipient must reject the entire message. In addition, the model developed in this paper should be strengthened to avoid the risk of reply attack.

,

## V. FACTOR AUTHENTICATION

**2**-factor authentication is the one of the best way to make secure of the soap massage .we will verify the Admin user as well as agent login.we also recorded the user as well as agent audit login time ,location and id of user too.In 2-factor authentication system send the token ID in mobile and email.it has 5 minute longer .after that it is not valid.random number is created for user and user verify the number and he/she will be able in.this is the 2-factor authentication security process.

## VI. ACKNOWLEDGMENTS

This work is partially supported by **Transcash International Pty. Ltd. (Trading as iPay)**
**| www.ipayremit.com**
An enterprise of iPay Financial Services Pte. Ltd.
77 High Street, #09-11 High Street Plaza, Singapore 179433
Office n(T): +65 6871 4272 Fax: +65 6871 4108,
**SINGAPORE | AUSTRALIA | HONG KONG**

## VII. REFERENCES

[1]. DavidChappell,Tyler Jewell, Java Web Services, O'Reilly, March 2002, 28-50.

[2]. Mark O'Neill et. Web Services Security, McGraw

[3]. Xiaoning Xu, "Security Study on transport of SOAP messages on Web Services", Information Security, 2011, No 11-3, Vol 22, 115-117.

[4]. "Analysis of Web Services Security", Micro-electronics and Computer, 2004.3, No3, Vol 21, 19-24

[5]. International Business Machines Corporation, Microsoft Corporation,VeriSign, Inc., Web Services Security (WSSecurity) Version 1.0, April, 2010.
Special thanks to https://www.c-sharpcorner.com/article/introduction-to-soap/
https://docs.oracle.com/cd/E26576_01/doc.312/e24945/soap-messages.htm#GMJVG001