The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.76 e-ISSN: 2251-7545

Enhancing Web Services Security in e-business

Iehab Alrassan
Computer Science department
King Saud University
Riyadh, Saudi Arabia
irassan@ksu.edu.sa

Maha Alrashed
Computer Science department
King Saud University
Riyadh, Saudi Arabia
Maha_al_rashed@hotmail.com

***Abstract*— Nowadays, most of enterprises are using Web Services as a new wave for exchanging information in their e-business integration. Security is a major concern when Web Services are emerged. Web Services are based on SOAP(Simple Object Access Protocol) message for exchanging information. In e- business, this information may be sensitive and there is a huge possibility that SOAP message is intercepted and modified by eavesdroppers.**

In This research, we discuss the significant impact of adoption Web Services in e-business, whereas Web Services support application-to-application interactions. However, security still the biggest challenge that faces Web Services. We also highlight the web services security standards that may be used to ensure Web Services security.

Any proposed security model must consider the securities' goals which are integrity, authorization, authentication, confidentiality and non- repudiation. In this research, we focus on SOAP message and how to ensure its security, since the SOAP message is the transmission unit in Web Services. We proposed a security model to enhance security of e-business. This model is based on XML signature and XML encryption to sign and encrypt SOAP message. Moreover, RSA is the encryption algorithm that used for encryption. We expect that our proposed model will achieve a good security with acceptable performance.

Keywords-Web Services, SOAP, e-business, XML encryption, XML signature, SAML, XKMS

I. INTRODUCTION

Today, Web Services is widely adopted in e-business. Web Service is a huge revolution in e-business, it changes the concept of application interactions from human-centric where client plays the main roles in interaction to application-centric which means application to application interaction.

Web Service is a key technology that supports easy integration, reusability, and dynamic e-business. In fact the major concern when Web Service is used in e-business is security. Web Service is related to many technology such as SOAP, WSDL, and UDDI. It uses SOAP message to transmit information, WSDL for describing the services , and UDDI for discovering services.

Web Service is based on SOAP (Simple Object Access Protocol) to exchanging messages between entities. SOAP protocol specification does not mention any security. Therefore, Web Services are vulnerable to various attacks. E-business Web Services security is mainly based on SOAP message. It uses SOAP message as a standard way to exchange XML data. Therefore, SAOP messages support the enterprise which uses e-business Web Services applications by making these applications accessible to other companies.

The challenge of the e-business Web Services is finding an appropriate mechanism to satisfy security requirements of e-business. For example, based on only SSL(Secure Socket Layer) cannot provide enough security because SSL is unable to achieve end-to-end security.

Secure SOAP message is one of the main goals of Web Services security. Attacker can be intercepted or modified the message. There are many standards to secure Web Services XML signature, XML encryption, WS-Security(Web Services-Security) ,SAML(Security Assertion Markup Language) and XKMS(XML Key Management System).

WS-Security does not provide any new technique, it is a combination of existing standards such as XML encryption, XML signature, and security tokens. SAML and XKMS provide the authentication and authorization. SAML is a standard used to exchange user security information assertion. Also, SAML provides Single Sign One (SSO).

XML signature and XML encryption are ways to sign and encrypt the whole or a portion of SAOP message. XML signature ensures integrity of message and guarantees that message is not tampered while XML encryption ensures the confidentiality of message. Encryption algorithm is a symmetric or an asymmetric. A symmetric cryptography for both sender and receiver use the same key while an asymmetric is composed of private and public key. The problem of a symmetric key is the key distribution, while an asymmetric key recovers this problem.

We proposed a model to secure Web Services based e-business. The security model considers both point-to-point security level and end-to-end security level. To achieve point-to-point security, we used HTTPS while to achieve the message level security we based on XML signature and XML encryption to provide integrity and confidentiality respectively. Also XML signature provides non-repudiation. We used RSA as encryption algorithm, the authors show in[1] and [2]that RSA has achieved a good performance.

The rest of this paper is organized as follow: Section II highlights the Web Services and e-business overview. Section III provides overview of Web Services Security standards , we discuss XML signature, XML encryption, WS-security, XKMS, and SAML. Section VI we present our proposed security model, we based on existing technologies to enhance Web Services security in e-business. Section I concludes the research and presents the future work.

II. WEB SERVICES AND E-BUSINESS OVERVIEW

Nowadays, most of enterprises used Web Services as a new wave in their e-business. There are a significant impact of adoption Web Services in e-business, whereas Web Services support application-to-application interactions

A. Web services

Web Services are software system that support and facilitate the program to program interaction over a network. The Web Services should be discoverable and describable. Many technologies are related to the Web Services, such as XML,SOAP,WSDL and UDDI.

- XML

XML provides many great advantages for transmitting data across the Internet.XML is a structure document. It is simple, independent, and extensible. These characteristics make XML adopted in many applications[3].

- SOAP(Simple Object Access Protocol)

SOAP is the most significant Web Services technologies. SOAP is a standard that exchanges message in XML format[3].Although SOAP protocol is used to exchange the messages in Web Services but this protocol does not describe the message format which is solved by defining the WSDL[3].

- WSDL (Web Services Description Language)

WSDL is XML-based format. It is a document that describes Web Services. WSDL is a guidebook for Web Services and contains information about what a service does and how user can access this service[4]. which is an XML-based, machine-generated, and machine-readable document that presents how to access to a Web Service.

- UDDI (Universal Description, Discovery and Integration)

The process where services requestor can discover the services provider and the description of the web services is called services discovery.

UDDI is registry standard, services requester will use it to search about services[4]. It stored data and metadata about Web Services, these information such that services location and how to invoke registered Web Services are contained in UDDI.

B. Web Sevices based E-business

Today many enterprises developed e-business system to carry out the business activities and make them more fixable and efficient [5]. E-business is defined as a electronically performing business activities , the business parties will interact by using networks or telecommunication technology In recent years, Web Services are adopted in a dynamic e-business.

The e-business functionality is divided into two models, the human-centric web and the application-centric web. Web Services move e-business to be the application- centric web and this make e-business more flexible, reusable, easy services integration[5].

In the human-centric web, the client plays significant role starting from initiating requests and finally gets the response. So, client is the main actors in e-business process. For example, when clients request goods from the e-shop to keep track with their request. They should log on e-shop site and check the status of their request via web browser, the result is as HTML page.

In application-centric, the clients role changed but the client still in the picture. The application is connected directly to services. In previous example, clients keep track of status of their order by themselves. However, Web Services can be used as order services application. This services collect the data, process it, and then return the result to client. The application-centric is very helpful in several areas such as credit card verification, package tracking, language translation, etc.

Web Services are the next step of internet based-application. The interoperability which is supported by Web Services, allows the applications implemented in different programming language and running on different platforms or operating system to communicate with each other.. Web Services specification does not define any security. To ensure Web Services security many efforts have been done to meet the Web Services requirement[6].

Most of Web Services based on SSL(Secure Socket Layer) to secure SOAP message. Actually using SSL does not provide enough security, there are many limitations of SSL:

1) SSL ensure only the point-to-point security.
2) SSL encrypts the whole message.
3) SSL does not sign the data.
4) SSL is inflexible routing because it is just Point-to-Point.

III. WEB SERVICES SECURITY

In Web Services SOAP message is a unit that exchange message. In e- business this information may be sensitive and there is a huge possibility that SOAP message is intercepted and modified by hackers. In next section we discuss the Web Services security standard that may be used to secure SOAP message.

A. XML Digital Signature

XML signature is defined by W3C. XML signature determines the representation of signed data in XML. XML signature allows selectivity which means user can signed whole document or part of it[7]. The signature is used to ensure the integrity of document and authenticity of the sender.

Digital Signature is a filter to make recipient sure that received message has not been tampered and it is an exact message from the sender[4]. The practical benefit of XML Signature is a partial signature which allows signing part of XML document by using specific tags. The XML Digital Signature can solve security problem such as spoofing and repudiation.

XML signature is a common method for ensuring the XML data integrity, authentication, and non-repudiation.

B. *XML Encyption*

XML encryption is defined by W3C. the confidentiality of message is provided by using XML encryption. Utilizing XML for representing encrypted web recourses (including XML data) is described by XML encryption specification. XML encryption specification distinguishes between encryption information and encrypted data and determines the encryption key information and encryption algorithm[3].

XML Encryption supports the selective as XML Signature which means the support of the encryption of portion of data. The selectivity property is very useful for Web Services security for example, in SOAP message certain information can be encrypted (Cipher Data) and hidden from hackers[4]. XML Encryption has many common points with XML Signature and it can be used with different data format.

C. *The XML Key Management Specification (XKMS)*

XKMS is W3C proposal. XKMS is support XML encryption and XML signature by determine a protocol that register, distribute, and process public key. is a PKI trust service that provides an XML interface to an underlying PKI.

Managing keys of XML encryption and XML signature will be simple by using XKMS. It is a simple Web Services to retrieve, validate, and register public keys. It provide easy way to manage the public key[3]. The XKMS performs two things:

1) Register public and this is done by XML Key Registration Service Specification (X-KRSS).
2) Rely on key to retrieve the information and this is supported by XML Key Information Service Specification (X-KISS).

D. *WS-Security*

In April 2002, IBM, Microsoft and VeriSign published a new web services security specification. WS-Security (WS-S) is a collection of the specifications and the framework used to ensure the security for XML[3]. WS-S defines how security tokens (a token is an XML representation of security information) are contained in SOAP messages. It also specifies how XML Security specifications are used to encrypt and sign these tokens, as well as how to sign and encrypt other parts of a SOAP message[4].

E. *Security Assertion Markup Language (SAML)*

SAML is XML language provides a solution for making security statement about user identity. The basic concept of SAML is assertion which is statements or claims about user. There are set of rules and syntax for exchanging user identity which is defined by SMAL. Business partners exchange user security information via SAML. The need to SAML is to provide portable trust which means a user whose already identified and verified in such domain has a right to use services in another domain(Single Sign On).

IV. PROPOSED SECURITY MODEL

Although there are many benefits of adopting Web Services in e-business, it affects by Web Services security. Web Services rely on exchange information via SOAP message. To secure SOAP message ,we must consider end-to-end security. Our proposed security model is consider both point-to-point and end-to-end security. We consider in our model the security goals and the performance of Web Services. We choose RSA encryption algorithm, [9][10] shows that RSA is very powerful and required less time rather than ECC or AES. RSA is rely on presuppose difficulty of finding factoring large number. In our proposed model we consider the performance of Web Services application.

We used XML encryption and XML signature thus we choose XKMS which is a best method to manage the requestor and provider key. XKMS ensures the authentication between requestor and provider.

We used XML encryption and XML signature thus we choose XKMS which is a best method to manage the requestor and provider key. XKMS ensures the authentication between requestor and provider.

SAML will be used to support SSO. We also ensure the security of SOAP message (request and response) we will signed request message to insure the integrity, and we encrypt the response message to ensure the confidentiality. The RSA algorithm will be used. We encrypt the response message because it contains the private information about the requestor. Fig.1 presents the proposed security.

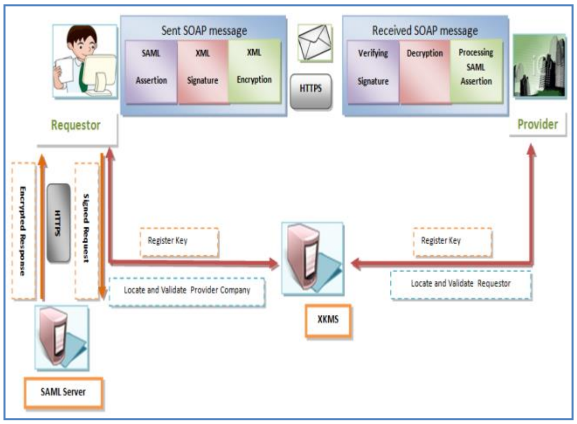

Fig.1 The Proposed Security Model.

A. Role design of Proposed Security Model

In our proposed method there are requestor, provider, XKMS, and SAML server. The requestor is the client who requests the services by sending SOAP message. The provider provides the services to the legal client. Services provider will verify the SOAP message and ensures that requestor has the access right to get the services. XKMS is important issue when XML encryption and XML signature are applied. XKMS is Web Services that register and locate keys for both the requestor and the provider. SAML assertion is provided by SAML server. The requestor logs in the SAML server which returns SAML assertion. SAML assertion consist of authentication, attribute, and authorization. Authentication assertion is responsible for ensures identity of user. Attribute assertion involves user information. Authorization assertion determines the access right of user.

B. Building the Proposed Security Model

First: XKMS server is used for registering public key of both company provider and requestor.

Second: client log in to system using SAML, using SAML provides single sign on. In this step we obtain SAML assertion.

- The authority will received a request from the requestor with username and password.
- The authority responsible about ensures the authentication of requestor, authority will create a document which contains SAML assertion.
- The authority returns SOAP message over HTTPS to requestor.

The requestor will be signed the SAML request using XML signature and send it to SAML server. The SAML server will be verify the identity of requestor, the SAML response will be encrypted and will be send again to the requestor.

Third: The requestor will decrypt SAML response. Then SAML assertion is included in SOAP header, this message will be send to the provider. SAML assertion contains authentication, attribute, and authorization. To avoid reply attacks problem the attribute security will be included in header of SOAP message. We add SAML assertion which contains the attribute timestamp and sequence number to SAOP request message to avoid the reply attack. SAML assertion will be signed.

Fourth: SOAP body is encrypted using XML encryption to ensure confidentiality. RSA algorithm will be used.

Fifth: SOAP message is signed using RSA algorithm.

Sixth: signed and encrypted message is transmitted through HTTPS.

When SOAP message is received provider company:

First: provider company check the validity of security attributes. If these attribute are valid then replied or denied.

Second: Verify the signature of SOAP message.

Third : Decrypt the SOAP message.

Fourth : Processing SAML assertion and ensure the identity of user to make a decision if there is response message or request will deny.

C. Analysis the Proposed Security Model

In our proposed model we consider point-to-point security and end-to-end security. Point-to-point security provides secure tunnel for transmitting SOAP message while End-to-end security ensures that SOAP message itself is not tampered or modified during the transmission.

Message level Security

XML encryption and XML signature can ensure end-to end security of SOPA message. SOAP message is signed and encrypted ,then is sent to company provider. Company provider receives SOAP message and verifies XML signature and decrypt XML encryption. If SOAP message is not tampered, company provider will execute the SOAP message and send reply SAOP message to client.

Authentication

Authentication has significant effect in e-business Web Services. E-business Web Services can be accessed by various enterprise. Therefore, we have to secure these Web Services and we make sure from authentication of the enterprise. Another important issue in e-business is single sign on. Single sign on let user to sign only one time to access resources without need to log in for each resource.

SAML, XKMS, and XML signature support authentication. SAML assertion is a ticket and the authentication of client is done by authority party not services provider. For e-business, SAML makes authentication management process is efficient because company do not have to do this process for companies which deal with them. XKMS is used to verify the identity of requestor and provider. XML security protect SOAP message from unauthorized access.

Data integrity

Integrity of SOAP message is achieved using XML signature. The way to prove that message is not modified by unauthorized user is used XML signature. Any changes made to the SOAP message is detected by validating the XML Signature. Thus, provider company ensures the integrity of data. When SOAP message is created the XML signature is generated and when SOAP message is processed the XML signature is verified.

Integrity of SOAP message is also achieved by using SSL, but it only does this while the message is in transit. When SOAP message is accepted by the next peer receiver, SSL connection is terminated. Therefore, we use both XML signature and SSL to provide integrity at message level and transport level. SSL is used to ensure point-to-point security, and XML signature provide end-to-end security at message level.

Confidentiality

Confidentiality of message is done by XML encryption. XML encryption is used to protect and preventing disclosure of the information from unauthorized users.

Non-repudiation

This property refers to the message sender cannot claim that message have not been sent. XML signature can achieved this goal.

Single Sign On

The SAML assertion is used to provide SSO. The user information is verified once time. Then user can use any services without need to log on another time.

V. CONCLUSION AND FUTURE WORK

The security is a challenging area in Web Services. Web Services can support interoperability of e-business and that refers to the nature of Web Services which is independent from any platform or operating system. Web Services support application-to-application which play significant role in e-business.

There are different standards to secure Web Services. XML encryption allows to encrypt part or whole message and ensures confidentiality of message. XML signature allows also the selectivity to sign whole or part of message. SAML provide SAML assertion which contains user information security. Using SAML provides authentication, authorization, and single sign on. XKMS is a Web Services, is used to manage keys of sender and receiver and support authentication and authorization.

Any proposed model must ensure the security goals integrity, confidentiality, non-reputation, authorization, and authentication. In our proposed model we use HTTPS to achieved point-to-point security. XML signature and XML encryption are used to ensure message level security. The RSA encryption algorithm will be used. [1, 2] shows that RSA algorithm is achieved a best performance.

SAML assertion is added to SOAP header to avoid reply attacks, it contains timestamp and sequence number. XKMS is used to support authentication and authorization of sender and receiver.

In our future work, we will apply implement our proposed model. We will build Web Services and we will applied our proposed model. We expect that the proposed security Web Services model will be secure and achieve a good performance.

REFERENCES

[1] S. M. Seth and R. Mishra, "Comparative Analysis of Encryption Algorithms For Data Communication," *INternational Journal of Computer Scince and Technology,* vol. 2, 2011.

[2] D. Rodirgues, D. F. Pigatto, J. C. Estrella, K. R. L, and J.C.Branco, "comparasion and analysis of crptographic algorithm aiming performance improvment in secure web services," in *proc.2011 IEEE 13th International Symposum on High-Assurance System Engineering*,2011.

[3] N. A. Nordbotten, "XML and Web Services Security Standards," Communications Surveys & Tutorials, IEEE, vol. 11 ,pp. 4-21, 2009.

[4] M. O'Neill, *Web Services Security*. Berekly,California: McGraw-Hill, 2003.

[5] M. Chen, "Factors affecting the adoption and diffusion of XML and Web Services standards for E-business systems," *International Journal of Humman-Computer Studies*, pp. 259-279, 2002.

[6] A. C. M. Chen, B. Shao, "The implications and impacts of web services to electronic commerce research and practices," *Journal of Electronic Commerce Research,* vol. 4, 2003.

[7] F. A. Kadir, " RewritingHealer: An approach for securing web services communication," M.A, Stockholm university ,Sweden, 2007

[8] Y. M.-t. Gu Yue-sheng, Gan Yong, "Web Services Security Based on XML Signature and XML Encryption" *JOURNAL OF NETWORK,* vol. 5.NO.9, 2010

[9] J. E. L. Kelly D.LEWIS, "Web Single Sign-On Authentication using SAML," *IJCSI International Jornal of Computer Scinesss*, vol. 2,2009

[10] D. Rodirgues, D. F. Pigatto, J. C. Estrella, K. R. L, and J.C.Branco, "comparasion and analysis of crptographic algorithm aiming performance improvment in secure web services," in *2011 IEEE 13th International Symposum on High-Assurance System Engineering*, 2011

[11] . M. Seth and R. Mishra, "Comparative Analysis of Encryption Algorithms For Data Communication," *INternational Journal of Computer Scince and Technology,* vol. 2, 2011.