Security Issues in Web Services: A Review Approach with process and applications of Multi–Part Multi-Signature Document

Abdul Jabbar Mohamed Hasmy

Department of Management & Information Technology
Faculty of Management & Commerce
South Eastern University of Sri Lanka
hasmie@seu.ac.lk

Abstract: Web Service is a new software technology that enables communication of various systems that are running on different platforms. The security issues of Web Services are a major concern of research due to its distributed environment. Web service security is one of the major areas of research both in industry as well as in academia. This current work is mainly bassed on security issues that are related with Web Services. The study is carried out with the common framework of security issues. Security issues that are special to web Services are discussed considering present available Web Service technologies. Use of Multi-Part Multi-Signature Document (MPMSD) in distributed environment is a current trend. The XML signature security also can be used with this approach. The application of Multi-Part and Multi-Signature Document related to security issues need to be further explored and experimented. Major purpose of this proposed work is to describe the process and applications of MPMSD in the distributed environment and study between XML signature security issues with the MPMSD. Furthermore, this work attempts to identify the future issues for research under MPMSD.

Key words: Web Service Security, Multi-Part Multi- Signature Document Web Services, Single-Sign-On, Digital Signature, XML Signature.

1. Introduction

1.1 Service Oriented Computing

Different Components can operate without worrying about the platform and language dependencies by using the latest technology called Service Oriented Computing (SOC) [7]. It is relatively a modern and interesting area. It facilitates effective ways to create and implement new distributed applications. SOC can be used to implement and configure distributed software applications in a manner that enables productivity and quality in great deal with service-orientation. Services are simply a way of building distributed applications over heterogeneous network, which emphasis on how services should function together and how these applications are built. SOC provides three main features: (i) description, (ii) discovery and (iii) communication. SOC native capabilities can be implemented using Web Service Description Language (WSDL) for description, Universal Description, Discovery Integration (UDDI) for discovery and Simple Object Access Protocol (SOAP) for communication. Web service is the current technology of SOC. Security is a major concern of services for service-oriented applications.

1.2 Service Oriented Architecture

A Service Oriented Architecture (SOA) is essentially a collection of services. These services communicate with each other. SOA defines an interaction between software agents as an exchange of messages between service requesters and service providers. Clients are software agents that request the execution of a service. Providers are software agents that provide the service.

The basic SOA is a relationship of three roles: a service provider, a service requester (consumer) and a service registry. The interactions involve publish, find and bind operations. The service requester uses a find operation to retrieve the service description from a discovery agency, and uses the service description to bind with the service provider and invoke the service or interact with service implementation.

1.3 Web Service

Web Services [9] are loosely coupled self- contained, self-describing and modular applications that can be described, published, located and invoked over a network. Web service can be provided on any platform and may be written in any programming language. Web Services essentially involve the three roles of SOA: service provider, service requester and service broker. A service provider could be an industry, business or a company capable of providing service. A requester also could be a company or a business that is in need of the service, whereas the broker is a place, entity or a system that helps both service provider and service requester to discover each other.

2. Web Service Model

The technologies that form the foundations of Web services are WSDL, SOAP, and UDDI.

2.1 WSDL

Functionalities of the services are described using Web Service Description Language (WSDL). When the requester receives the WSDL document for the particular Web service, it must be first validated. This can simply achieved by incorporating a digital signature of the WSDL document for the requester to use. Without some way of authentication requesters cannot connect to most providers. WSDL v1.1 does not provide internal mechanism for signing WSDL documents. WSDL v1.1 does not provide a method for specifying the security requirements of a Web service. Future versions of WSDL are expected to have this feature.

2.2 SOAP

Simple Object Access Protocol (SOAP) is used for communication among different Web Services. SOAP [4] messages flow from originator to an ultimate receiver through a SOAP message path. A SOAP message consists of Soap: Envelope which contains a Soap: Body element and an optional Soap: Header element. The Soap: Header element may contain a set of child elements that describe message processing that the sender expects a recipient to perform.

```
<Soap: Envelope>
<Soap: Header> (optional)
<Soap: Body> (mandatory)
<get Quote symbol = “——”/>
</Soap: Body>
</Soap: Envelope>
```

Example 1: A Simple SOAP message.

- SOAP envelope is used for encapsulate the SOAP message.
- SOAP header is the optional part of the SOAP protocol. Header contains information for the SOAP node, the processor of the SOAP message, how to process the SOAP message. This may be authentication, routing etc.
- Soap body contains the targeted to the SOAP message receiver.
- Get Quote element is the child of SOAP body.

2.3 UDDI

Universal Description Discovery and Integration (UDDI) is mainly a registry of Web Services used to register all of the information for a Web Service. This includes publishing and discovery information of the Web Service. UDDI service can be considered as an industry-wide effort to bring a common standard for business- to-business (B2B) integration. It has a set of standard interfaces to access a database of Web services. The UDDI allows users to discover available Web services and interact with them dynamically. The process can be divided into three phases: (i) Searching (discovery), (ii) Binding and (ii) Executing [11].

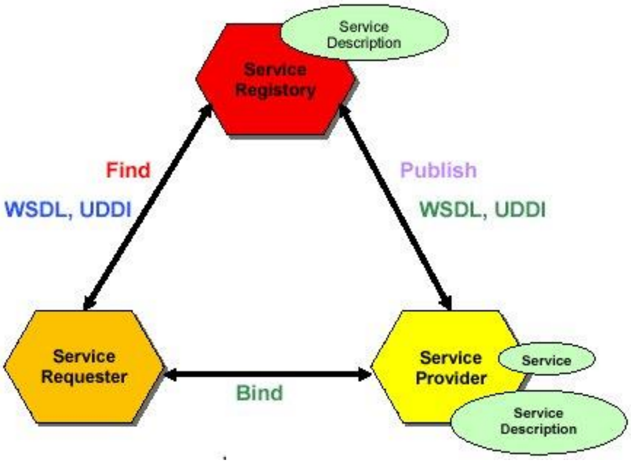


Fig. 1. Web Service Model

Web Service is an attractive and powerful technology for development of distributed application as well as for integration. But for wide acceptability by the developers and consumers in Business-to-Business (B2B) and Business-to-Consumers (B2C) scenarios, it must be secured. Therefore, study of security issues in Web Services is a need of the hour.

3. General Security Framework

Security in any system can be studied under a common general framework. Web Service is not an exception. The framework consists of the following issues.

3.1 Authentication

Authentication is concerned with the establishment of the proof of identities of entities in a system. The entity may be a user, a process or a service. Masquerading is a standard attack in authentication mechanism.

3.2 Authorization

Once an entity has been authenticated, the next issue is to ascertain which operations the entity is allowed to do and on what resources. The authorization mechanism deals with granting and revoking privileges of authenticated entities.

3.3 Confidentiality

The issue of confidentiality specifies that only the sender and the intended recipient should be able to access the content of the message. An unauthorized person should not be able to access a message. It is achieved by encryption and decryption of messages. An encryption algorithm is used to convert plaintext into cipher text. There are two types of encryption in general use: symmetric and asymmetric encryption. In symmetric encryption, the decryption key is the same as the encryption key and in asymmetric encryption; the decryption key is not same as the encryption key. Eavesdropping is a standard attack in confidentiality.

3.4 Non-Repudiation

There are situations when a user sends a message, and later on repudiates it. Repudiation may be on sending, receiving or on the time of sending or receiving the message as well.

3.5 Availability

The issue of availability states that resources, services should be available to authorized parties at all times. Denial of Service (DoS) is a standard attack on availability.

3.6 Integrity

When the content of a message is changed during transmissions than the integrity of the massage is lost. Data integrity relies on mathematical algorithms known as hashing algorithms. A hashing algorithm takes a block of data as input and produces a much smaller piece of data as output. This output is called a digest of the data. If the data is a message, it is called a message digest. MD5 and Secure Hash Algorithm (SHA) are the standard hashing algorithms.

4. Special Security Issues for Web Services

Under the general framework discussed in section 3, special security issues related to Web services are discussed as follows:

4.1 Authentication for Web Services

In SOA, the three roles: requester, provider and registry need to be authenticated during composition, binding and execution of Web Services. When a new service is composed using existing services, the descriptions of which are provided by the registry, then the registry is to be authenticated by the requester. Moreover, if it is not a public service, the requester may be required to be peer authenticated by the registry. Similarly, during execution of services also, the requester and the provider may need to peer-authenticate each other. Web Services may be vulnerable to man-in-the attack, masquerading attack during composition, binding and execution.

Another relevant issue is how to ascertain that the description of the service provided by the registry and the actual service provided by the provider for binding are the same. Some sort of certification of this association between description and the actual service is required. Can the registry role also apply certifying authority in this case? If so, it can be a Trusted Third Party (TTP). But whether off-line, on-line or in-line TTP needs further investigation.

Authentication Techniques

Single-sign-on: Once the end-user has been authenticated by its attributes login-id and password, it needs to be authenticated again for communicating with the other services. Once the end-user signs on to a web site and then a SOAP request is produced on the user’s behalf, the route among multiple Web Services is established using user’s login-id and password. This functionality is known as Single-sign-on.

Federated-trust: Once the end-user has been authenticated using its attributes login-id and password, the route among multiple Web Services may be established on the basis of their trust relationships. This mechanism is called Federated- trust.

WS-Trust: To route among multiple Web Services and the trust relationship must be established among different services. The trust relationship among multiple services can be either direct or brokered.

Service Authentication

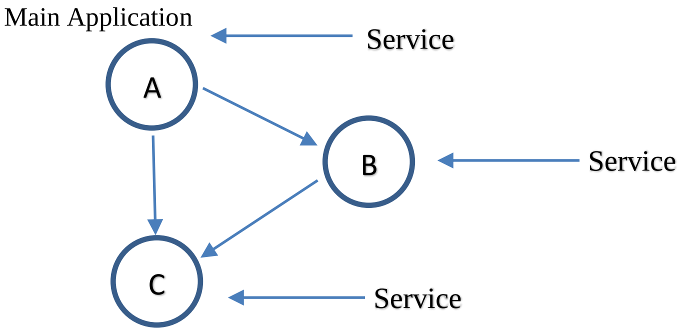


Fig. 2. An example of Multi-hopping.

Let us assume,
service$_A$ authenticate service$_B$=>service$_A$ trusts service$_B$,
service$_B$authenticate service$_C$=>service$_B$ trusts service$_C$,
Therefore, service$_A$ authenticates service$_C$ => service$_A$ trusts service$_C$.

The above example shows the case of Multi- hopping, which means that the route through multiple Web Services. This also depicts the concept of WS-routing, where SOAP message is to route through multiple Web Services. The concept of WS-routing is not same with Single- sign-on and Federated-trust, because the former considers only the SOAP messages has to route among multiple Web Services whereas the later are based on authentication and trust establishment among multiple Web Services. So far security challenges are concerned, the security mechanisms like Single-sign-on and Federated- trust may be designed on the top of WS-routing.

4.2 Authorization for Web Services

An authorization decision is needed for the destination Web Services for getting information about the end-user who signs once for routing the SOAP request among multiple Web Services. When multiple web services are being run in quick succession and time is of the essence, it is important that the overhead of authorization not occur each time another web service is being run. SAML (Security Assertion Markup Language) and XACML (eXtensible Access Control Markup Language) are the two technologies that are used to ascertain authentication and authorization information. The access control mechanism deals with two techniques namely, Role Based Access Control (RBAC) and Context Based Access Control (CBAC).

4.3 Confidentiality for Web Services

In the world of information security, the term confidentiality is used to refer to the requirement for data in transit between two communicating parties not to be available to the third parties that may try to interrupt in the communication.

XML Encryption is the technology used for confidentiality in Web service security. It acts as the basis for other security technologies such as XML signature. General proof of origin security requirements of Web services may be addressed by XML signature available today. But for certain security requirements in workflow environment, like multi-signature and multi-part multi-signature the present version of XML signature may have limitations.

4.4 Non-Repudiation for Web Services

Digital signature is not sufficient for non-repudiation protocol. Fair non-repudiation protocol and its variants need a central arbiter as a TTP. This may be a bottleneck for future secure of Web services. For public Web services, non- repudiation may not be a major issue. But the formal Web services of e-Governance and commercial services against payment, non-repudiation is one of the major issues to be addressed. XML signature is the technology that can be also used for non-repudiation protocol.

4.5 Availability

Availability is a major issue in Web service security. One of the means of denying availability is due to the DoS attack. A DoS attack aims to use up all the resources of a service so that it is unavailable to potential users.

4.6 Integrity

Integrity of Web service is mainly concerned with the WSDL file, which describes the functionalities of a Web service. When a service requester communicates with the registry for a suitable service, WSDL file is the basis of selecting the service during composition.

But if it is tempered during transit or storage it may provide misinformation, which is a lead to rejection of the service during composition and malfunction as well as during execution of the service. XML signature is the technology that can be used for message integrity.

5. Discussion on Present Technologies

WS-Security: WS-Security is a building block that intended to be used in conjunction with other Web Services and application specific protocols to accommodate a wide variety of security models. WS-Security [4] does not claim to provide a complete solution to securing Web services. The XML signature and XML encryption specifications provide standard methods for digitally signing and encrypting XML documents including SOAP messages. Not only can whole documents be signed or encrypted, but also individual parts. WS-Security defines how XML signature data can be included in a SOAP message. This provides persistent confidentiality beyond a single SOAP communication.

Secure Socket Layer: Secure Socket Layer (SSL) is a protocol or technology, which is used to protect companies from web Service Security attacks. SSL used in encryption technique, which are in turn used to implement for data protection. SSL creates a secure tunnel in between originator and destination computers based on public key encryption technique. A common protective measure is to send messages over a secure connection that is using SSL. For example, an SSL connection between two points may be sufficient for simple applications. For multiple Web Services, complete message or individual part of messages may be encrypted and signed to protect the confidentiality and integrity of Web Service messages [5].

XML Encryption: XML Encryption provides end- to-end security for applications that require secure change of structured data. XML Encryption is mainly ensuring confidentiality to encrypt the XML data. XML based Encryption is the natural way to handle requirements for security in data interchange applications. XML Encryption is not intended to replace or supersede Secure Socket Layer (SSL). Rather, it provides a mechanism for security requirements that are not covered by SSL. XML encryption is ideal for confidentiality. XML Encryption does not introduce any new cryptography algorithms or techniques. RSA Encryption may still be used for actual encryption.

SAML: Security Assertion Markup Language is a protocol for asserting authentication and authorization information. It also provides attributes of an end-user in XML format. It allows information to be placed on a SOAP message. SAML servers can be accessed for authentication and authorization data in order to enable Single-Sign-On (SSO). If the recipient of this SOAP message trusts the sender of the SAML data, the end user can also be authorized for the Web Service.

XACML: eXtensible Access Control Markup Language or XML-Access Control Markup Language (XACML) is designed to express access control rules in XML format. Although the two technologies are not explicitly linked, XACML may be used in conjunction with SAML. An authorization decision expressed in a SAML assertion may have been based on rules expressed in XACML.

6. Contribution

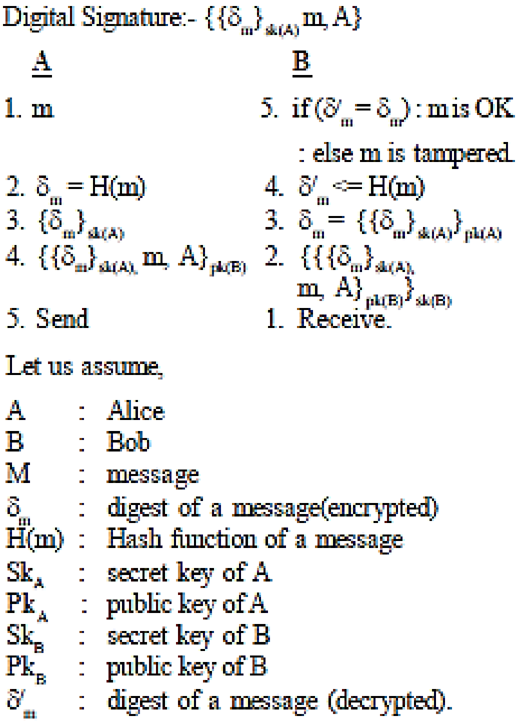
The main aim of this paper is to do the review work on general security issues and special security issues of WSS. From the investigation, it is found that service authentication can be incorporated as a new item of special security issue in security mechanisms like WS-

Routing and Multi-hopping. Also some new security issues have been highlighted in this paper along with discussion on security mechanisms like federated trust, single-sign-on and WS-trust. The remaining sections of this paper are organized by the discussion on present technologies and a probable solution of the problem has given on discussing some other technologies like digital signature, XML signature and MPMSD. Finally, discussion is concluded with some future directions.

7. Proposed solution

The main objective of this paper is security issues in Web services and accordingly discussed a common framework of general security issues. Also, discussed some new security issues in Web Service Security (WSS) along with their attacks. The following are some technologies which can give an optimum solution of security mechanisms.

Digital Signature [2]: It is independent of the signer's name and handwritten signature.



Digital Signature:- $\{\{\delta_m\}_{sk(A)} m, A\}$

A	B
1. m	5. if ($\delta'_m = \delta_{mr}$) : m is OK : else m is tampered.
2. $\delta_m = H(m)$	4. $\delta'_m \Leftarrow H(m)$
3. $\{\delta_m\}_{sk(A)}$	3. $\delta_m = \{\{\delta_m\}_{sk(A)}\}_{pk(A)}$
4. $\{\{\delta_m\}_{sk(A),} m, A\}_{pk(B)}$	2. $\{\{\{\delta_m\}_{sk(A),} m, A\}_{pk(B)}\}_{sk(B)}$
5. Send	1. Receive.

Let us assume,

A	:	Alice
B	:	Bob
M	:	message
δ_m	:	digest of a message(encrypted)
H(m)	:	Hash function of a message
Sk_A	:	secret key of A
Pk_A	:	public key of A
Sk_B	:	secret key of B
Pk_B	:	public key of B
δ'_m	:	digest of a message (decrypted).

XML Signature : XML Signature is a protocol that describes the signing of digital content. The XML Signature standard includes protocols for signing sections of XML documents. XML signature enables such capabilities as message integrity. XML Signature provides integrity for data. XML Signature is also important for authentication and non-repudiation. XML Signature is a technology that must be implemented correctly if it is to be a valid security tool. XML Signature may also be used for integrity and non-repudiation of WSDL files so that the definition of Web Service can be published and later trusted. XML Signature provides a useful means of expressing a Digital Signature over XML data.

The structure of an XML signature is:

```
<signature>
   <signedInfo>
      (canonical form) — to avoiding white space.
       (signature form)
            (<reference(URI=) ? >
            (transforms) ?
               (digest method)
               (digest value)
            </reference>) +
    </signedInfo>
   (signature value)
 </signature>
```

Where, ? => 0 or 1 time, + => 1 or more time, *=> 0 or more time which has taken from the concept of regular expressions.

Multi- Part Multi-Signature Document (MPMSD)

Document production in an office is based on a request-reaction-response paradigm. A Multi- Part Multi-Signature Document (MPMSD), D_W, produced in a Document Production Workflow (DPW) W, is an n-tuple, n=1, such that $D_W = (d_1, d_2, d_3,- - -, d_n)$. Each part d_i in turn is defined as a 3-tuple (m_i, σ_i, s_i), where m_i is the comment of the reviewer s_i, and σ_i is the signature of s_i

A Scenario

In an office system, a worker called the originator, creates a document and sends it to another worker, who reviews, gives comments and forwards it to another worker and so on. This process in reply will give a composite document, composed of list of comments, contributed by the originator and the reviewers during the process. This type of document is called as Multi-Part Multi-Signature Document (MPMSD). The above mechanism of MPMSD is shown in the Fig. 3.

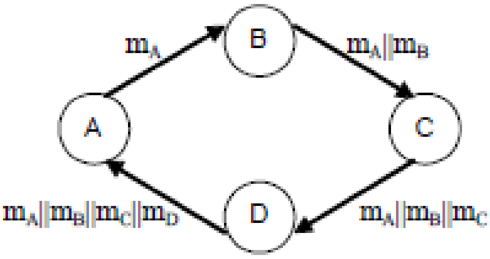


Fig. 3. Mechanism of MPMSD

In a manual system, it is the same paper document that is passed around and the proof that it has come through the proper channel with the addition of series of comments followed by the signatures of the reviewers.

8. Conclusions and Future Work

In the present work, a review of security issues in Web service is done under a common security framework. In this paper, some new security issues are highlighted. The technology like WS-Routing can be applied on SOAP messages for secure multi-service hopping. While reviewing the literature, it is found that data mining techniques can be used effectively for detecting attacks.

A new security architecture based upon Web services that support authentication, authorization and federation is a central point for future research. Also whether XML signature and MPMSD provides security to data and contents are also points for future enquiries.

References

[1] D. Cotroneo, A. Graziano, S..Russo. “Security Requirements in Service Oriented Architectures for Ubiquitous Computing”. 2nd Workshop on Middleware for pervasive and Ad-hoc Computing. Toronto. Canada, 2004

[2] K. N. Gupta, K.N Agarwala, P.A Agarwala, Digital Signature: Network Security Practices. PHI Pub. New Delhi, 2005

[3] C. Gutierrez, E.F. Medina, M Piattini, Web Services Enterprise Security Architecture: A Case Study. Fairfax. Virginia. USA,2005

[4] A. Kahate, Cryptography and Network Security. TATA McGraw Hill, 2003

[5] P. Kearney, J. Chapman, N. Edwards, M. Gifford, An Overview of Web Services Security. BTtech. Journal. 22(1): 27-42, 2004

[6] M. Mcintosh, P. Austel, XML Signature Element Wrapping Attacks and Countermeasures.Fairfax. Virginia. USA, 2005

[7] N.H Michael, M.P Singh, Service-Oriented Computing: Key concepts and principles. IEEE Internet computing. 9(1):75-81, 2005

[8] N. Milanovic, M. Miroslaw, Current solutions for Web-Service Composition. IEEE Internet Computing: 51-59, 2004

[9] M.O Neil, Web-Service Security. Tata Mcgraw Hill Pub. New York, 2003