A Framework for the Model Driven Development of Secure Web Services Composition

Muhammad Qaiser Saleem, Jafreezal B. Jaafar, Mohd Fadzil Hassan

Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, 31750, Seri Iskandar, Perak Darul Ridzuan, Malaysia.
muhammad.qaiser.saleem@gmail.com, jafreez@petronas.com.my, mfadzil_hassan@petronas.com.my

Abstract

Now a day’s enterprises are implementing their WIS using web services technology by composing the web services. They are using the MDA approach to develop the WIS and UML is used as a modelling language for business process modelling. Security is not defined during the early phases of WIS development i.e. during designing the service composition and left to developers. Properly configuring security requirements for service composition is quite difficult for developers because they are not security experts; furthermore, service composition’s security is cross-domain and all required information is not available at downstream phases. A Model Driven Security framework is proposed for the development of secure web services composition; where along with the business process modelling, using the UML Activity diagram, business domain expert also model the security objectives. Adding security during the design phase helps to save the time and effort during the implementation and verification of security in the SOA applications. Furthermore, specifying security requirements at abstract level, help the architectural team in choosing the different and potentially better security mechanisms. As a proof of work the proposed framework is applied to a typical business process of healthcare domain.

Keywords: Service Oriented Architecture, Services Composition, Business Process Modelling, Security Goals, Model Driven Security, Domain Specific Language

1. Introduction

Today’s Information Technology (IT) environment is a network/Internet centric such as Service Oriented Architecture (SOA), Cloud and SaaS (Software as a Service) which offer the IT agility demanded by the business [1, 2]. In SOA environment, software applications are deployed over the Internet as a service. To support a business ventures, these services are integrated/composed within and across organizations to form Internet-based systems and perform cross application transactions [3]. The paradigm of SOA promises inter-operability and integration ensuring the availability of resources in the form of services over the network. SOA is an architectural style in which software applications are comprised of loosely coupled reusable services by integrating these services through their standard interfaces. Services are independent of language, platform and location and may be locally developed or requested from the provider. A business process can be realized as a runtime orchestration of set of services. Software applications are often comprised of numerous distributed components such as databases, web servers, computing nodes, storage nodes etc. and these components are distributed across different independent administrative domains. Services are used but not owned by the user and they reside on provider side [4-6]. SOA is also called a “Find, bind and invoke paradigm” [3, 7].

Currently most for the enterprises develop their Web Information System (WIS) using web services technology by composing web services which may be graphically located at different sites using SOA paradigm [8]. The area of web services composition has gained an interest in the web service community, however most of the research work addresses implementation and execution issues therefore many composition languages are proposed in recent years such as BPEL (Business Process Execution Language), XLANG (X Language), WSFL (Web Services Flow Language) and WSCI (Web Service Choreography Interface) etc. are among few of them. However these languages are not related to the early stages of the system development [9]. Furthermore, few methods/frameworks [9-12] are
presented for service composition; however notion of security is neglected in almost all of them i.e. security is not defined during the business process modelling of SOA applications.

SOA environment is full of daily virus alerts, malicious crackers and the threats of cyber terrorism [1, 2]. With the increase in number of attack on the system, it is probable that an intrusion can be successful [13]. The security violation defiantly cause losses, therefore it is necessary to secure the whole system. Security must be unified with the software engineering process and the business process modelling is the most appropriate layer to define security [8]. However, in practice security is considered afterthought and implemented in ad-hoc manner [14]. Furthermore it is left to the developer and added when the functional requirements are met or at the time of integration of distributed applications which is not a realistic approach [15]. Service compositions are cross-domain and coupled over various network technologies and protocols; just adding security code to software applications is not a realistic approach because all required security information are not available at the downstream phases[15, 16]. This approach degrade implementing and maintaining security of the system [17].

A Model Driven framework is proposed for web service composition where, security objectives are defined for services composition while performing business process. This security annotated business process model will automatically transform into a service composition using Model Driven approach. Now the focus is different, to compose an advanced service (service composition) out of basic atomic services. Security objectives are defined initially for atomic services and afterwards for the composed advanced service. We are proposing a framework for the model driven development of secure web service composition, where along with the business process modelling, using UML activity diagram, business domain expert also model the security using Domain Specific Language (DSL) presented by different authors like [14, 18-22]. During this research work, UML-SOA-Sec [21] is used for the modelling of security objectives. Proposed work is projected to the real world example of healthcare systems.

2. Related Work

Related work is presented in the area of web service composition where different authors have presented different frameworks/methods for service composition.

Bart Orriëns et al. [23] has presented a phased approach and named it as “Service Composition Life cycle” and four broad phases are described for service composition naming definition, scheduling, construction and execution. It is a general framework just describing the whole process of service composition. Roy Grønmo and Ida Solheim [11] described the whole process of web service composition by naming it as “Actions to build a composite web service”. They emphasize that for service composition modelling one should perform two kind of modelling: the service and the workflow modelling. Service modelling identifies services to be exposed with their interfaces and operations (UML Class Diagram); while the workflow modelling identifies the control and data flows from one service to the next service (UML Activity Diagram).

“UML-S” (UML for Service) is presented by Christophe Dumez et al [9]. They defined the static aspects of the composition i.e. interface of the Service Composition by UML-Class diagram (WSDL interface and data types involved), and used the UML-activity diagram to model the dynamic aspects (The composition scenario itself, i.e. the interaction between the existing services). Christophe Dumez et al. [24] presented the different steps under the titled as “Composite Web Service Development Process” which should be performed for the web service composition. Christophe Dumez in his PhD dissertation [25] presented a framework for Service Composition based on these steps.

Skogan et al. [12] is presented an approach where service composition is modeled using the UML activity diagram. They propose a “a method, a UML profile and transformation rules” that can be used to produce UML models of web service compositions that are executable. They have provided a way to model the coordination and the sequencing of the interactions between Web services. However, in this approach, methods, input/output and data transformation are modeled as notes (i.e. comments) on the side of the workflow, which can get quite confusing when the composition flow gets complex.

Limitation of all of the above mentioned Frameworks is that they do not treat security as a separate activity. Jun Hall et al. [3] have presented a framework naming “Security-Oriented System
Composition and Evaluation" they defined the security objective along the modelling at two level i.e. at system level as well as at service level.

During this work, security objectives are defined along service composition modelling, which is performed using the UML activity diagram at two different stages; however we do not differentiate them as system level and service level it is business process modelling

3. Foundational Concepts

3.1 Service Oriented Architecture and Web Services

SOA paradigm makes the application development easy by coupling services over intranet and via the Internet [15]. SOA paradigm has changed the Internet from being repository of data to repository of services [26]. SOA is an architectural style in which software applications are comprised of loosely coupled reusable services by integrating these services through their standard interface. Services are independent of language, platform and location and may be locally developed or requested from the provider. A business process can be realized as a runtime orchestration of set of services.

The basic building block of a SOA paradigm is a service. Web services technology is a widespread accepted instantiation of SOC which should facilitate integration of newly built and legacy applications both within and across organizational boundaries by avoiding difficulties due to different platform, heterogeneous programming languages etc. They enable dynamic connections and automation of business processes within and across enterprises for Enterprise Application Integration (EAI) and Business-to-Business (B2B) integration [27]. Basic idea behind Web Services technology is to exploit the Internet and XML technologies and to develop the applications by integrating web services which are published, located and invoked over the web. Web Services are defined as “self-contained, modular units of application logic which provide business functionality to other applications via an Internet connection” [27]. Basic standards for the Web services technology are SOAP (Simple Object Access Protocol), WSDL (Web Services Description Language) and UDDI (Universal Description Discovery and Integration). These all three standards are XML based [27].

3.2 Web Services Composition

To implement business collaborations, web services provided by different vendors can be interconnected, which leads to Composite Web Service. Composed services are provided by gluing together the WSDL services and corresponding operations. Currently business logic of the composite web service is expressed with the help of a business process modelling language like UML [28].

Simple interaction among the web services using standard messages and protocols is not sufficient in the case where business processes are integrated across enterprise boundaries [27-29]. Real business scenarios involve long-running interactions, transactions management, state-full invocations and are often driven by a workflow engine [27]. This raises the need for web services composition languages that provides the mechanism to fulfill the complexity of business processes execution [27, 28].

3.3 Web Services Composition Languages/ Standards

Web services composition languages are built directly on top of WSDL[28]. Two different communities are working for advancement in web service compositions namely: 1) the Business Process Management (BPM) community; and 2) Workflow community [12].

3.3.1 The BPM community:

This community has mainly focused on web service technology and has come up with a multitude of web service composition standards [12].

The most popular language for web service composition is BPEL4WS (Business Process Execution Language for Web Services) or simply called as BPEL (Business Process Execution Language). BPEL is built by combining IBM’s WSFL (Web Services Flow Language) and Microsoft’s XLANG (Web Services for Business Process Design). XLANG is a block-structured language while WSFL is graph-
oriented language [28]. BPEL is presently a working draft by OASIS (Advancing Open Standards for the information Society). BPEL is used for the “Orchestration” of the Web services [27].

BPML (Business Process Markup Language) is the standard proposed by the BPMI (Business Process Management Initiative). BPML was originally developed to enable the standard-based management of e-business processes used with BPMS (Business Process Management System) technology. However it can be applied to a variety of scenarios, including EAI (Enterprise Application Integration) and Web services composition. BPML is a specification language committed to executable business processes [27]. BPML and BPEL4WS are quite similar and are now being merged in OASIS [12].

World Wide Web Consortium (W3C) presented WS-CDL (Web Services Choreography Description Language). WS-CDL models the peer-to-peer collaboration between participants with different roles using “Choreography” [27]. Other proposals are HP’s Web Service Conversation Language (WSCL) and SAP/Intalio/Sun/BEA’s Web Service Choreography Interface (WSCI) [12].

3.3.2 The Workflow Community:

This community is working outside domain of web services and focused on established technologies which are now extended with web service capabilities. They also support different forms of composition languages. The Workflow Management Coalition (WfMC) provides a specification for interchange of composition models called the XML Process Definition Language (XPDL) [12].

There are many more standards for web services composition one can find in literature. Abundance of these overlapping standards is overwhelming. “In fact, the collection of competing web services standards without clear added value has been termed the Web Services Acronym Hell” [28].

4. Proposed MDS Secure Web Services Compositions Framework

In the proposed MDS services composition framework; the most important steps are selected among those steps discussed by different researchers. The main contribution is the definition of security objectives along business process modelling, which is performed using the UML activity diagram at two different stages i.e. at step-1 and step 3. The proposed DSL “UML-SOA-Sec” is used for security modelling. The proposed framework identifies the steps where the business process expert has to model the security objectives along the business process modelling for services composition. This security annotated business process model will be transformed into a services composition using a model-driven approach. Now the focus is to compose an advanced service (services composition) out of basic atomic services.

The principle of the MDS services composition framework is to use the UML to model the services composition and from the UML models, to generate the BPEL model and WSDL specification. In the area of web services composition research, there are two main aspects that are modelled: the service and the workflow. Service modelling identifies services to be exposed with their interfaces and operations, (a UML Class diagram is used for service modelling) while the workflow modelling identifies the control and data flows from one service to the next (a UML activity diagram is used for workflow modelling) [11].

A web service is represented by UML class diagram, which may consist of several operations that are represented by the operations of the UML class diagram. Each individual operation has its own internal behavior, which is expressed by the UML activity diagram. The UML activity diagram prescribes the implementation of the operations with the help of a structured set of activities called composition, which describes the control flow and data flow among the activities. An activity in the UML activity diagram corresponds to the invocation of a web service operation. A composite web service has one or more operations which invoke basic web services [30].

The goal of the framework is to design secure web services composition using the UML activity diagram. The four steps presented in the framework are already defined for web services composition e.g. Roy Grommo and Ida Solheim [11], Christophe Dumez et al. [31, 32], Skogan et al [30], Jun Han et al. [3] and Andre R.R. et al.[33]. The contribution of this research work is the defining of the security in the UML activity diagram at step-1 and at step-3 with the help of the proposed DSL “UML-SOA-Sec”.

A Framework for the Model Driven Development of Secure Web Services Composition
Muhammad Qaiser Saleem, Jafreezal B. Jaafar, Mohd Fadzil Hassan
The following is a detailed description of the proposed model driven security framework for services composition as described by Figure 1.

**Figure 1. Framework for Model Driven development of Secure Web Service Composition**

**Step 1: UML Modelling of Service Composition:**

The goal of this step is to perform modelling for the composite application and to identify the candidate web services. At the preliminary stage, two kinds of modelling are performed: firstly, the UML class diagram is modelled to describe the interface of the proposed composite web service. Secondly, the UML Activity diagram is modelled to show the sequence of operations to be performed and the control flow of the proposed services composition. The security objectives in UML Activity diagram are incorporated by using the “UML-SOA-Sec”, which will result in a security annotated UML activity diagram. Web services are identified by their names and textual descriptions in the UDDI registry, but their operations are described in the WSDL files. The business process expert (modeller) has to search, discover and extract the WSDL description of the web services from the web service repository, which is placed on the Internet server.

**Step 2: Transforming of WSDL of discovered Web Services into UML Class Diagram:**

The goal of the second step is to model the details of the services composition. The business process expert (modeller) transforms the WSDL description of the extracted web services into a UML class diagram. At this stage, the basic services are identified that are used to generate the UML class diagram of the services composition which will serve as the interface for composite web service.
Step 3: Refining UML Activity Diagram of Composite Web Service:

During this step, refining of the UML Activity Diagram of the composite service is achieved by adding the details found in the WSDL description of the web services. It will define the internal behavior of the services composition. Refinement of the security objectives is also achieved and preparation of a security enhanced UML activity diagram for the services composition.

Step 4: Transforming of UML Models into WSDL and BPEL:

During this step, UML models are transformed into a code. At the end of this step, the composed service is ready for deployment. The UML Activity diagram will be transformed into an executable specification like the BPEL and its specification will be deployed on a work flow engine which produces an implementation code for handling control-flow and data-flow. The UML Class diagram is transformed into a WSDL description which would be published in the Web Service repository. Once the web service is published in the registry, it can be discovered and used by the web service consumers.

Discussion

The main contribution in the proposed MDS services composition framework is incorporating security objectives for modelling of the services composition. In the proposed framework, security is defined at two different stages. Firstly, at step-1, the overall modelling of the services composition is performed using the UML activity diagram. This is the concept building stage about services composition i.e. what functionality this services composition has to perform and which services are required to accomplish this functionality. Secondly, at step-3, all required services are either discovered or developed; now all the required services are available and security will be refined/redefined for modelling of the services composition using the UML activity diagram. During this work, “UML-SOA-Sec” is used for security modelling.

5. Evaluation of the Proposed MDS Web Services Composition Framework

This paper claims contribution in the area of Web Service Composition by providing a framework, which is implemented with a case study, presented in this section. Initially; security enhanced business process model is presented which is modeled in UML Activity diagram. Later on, this UML activity diagram is transformed into a BPEL workflow.

5.1 Security Enhanced Business Process Modelling of Web Service Composition

In SOA environment, the system is composed of the services offered by different partners. These services from different partner organizations are integrated to form application and every organization work independently without central control. The distributed nature of SOA environment and technology-heterogeneity of the services, raise many security challenges. The inter-organizational workflow in SOA environment is executed in a decentralized manner where one need to secure local data stores as well as the communication among the partners [34]. In such environment different use cases can be derived from the scenario to model the business process and then define the security requirements. For our research work we are focusing the SOA based healthcare scenario.

5.2 Security Objectives of Healthcare Systems

Healthcare data is stored at healthcare partners e.g. diagnostic lab, clinic, pharmacy, insurance company etc.; therefore providing security and privacy to the medical data is the key responsibility of the healthcare applications. For better care and appropriate diagnostic, timely access to the medical data by the authorized user is very essential. The system should prevent the disclosure of medical data to un-authorized users who can exploit it for criminal or commercial use. Therefore Confidentiality and Integrity of the data should be ensured by the system; which is technically ensured through proper Access Control mechanism. Access Control itself is ensured through “Authentication” and
“Authorization” mechanisms. Partner organizations make sure that only authenticated and authorized users with specified permission would access the medical data. In a simple scenario different users in healthcare organizations like primary physician, medical specialist, radiologist, insurance personal etc. are assigned certain roles based on their organizational responsibilities to access the medical data. These roles are assigned certain credentials through which they are identified and after proper authentication and authorization checks they are allowed to use healthcare data and services.

Healthcare scenario involves sending and receiving of several documents. It is important, once a particular document is sent or received; one should not be able to deny having sent or received the document. If a user access the data or a service then for the evidence the system should log the details of this access event; therefore accountability of accessing the data is also an important security requirement which is achieved through “Non-Repudiation” mechanism which create signed evidence for accessing the system resources [34]. Non-repudiation ensures accountability regarding access to healthcare documents and services.

5.3 Healthcare Security Scenario

Realizing the importance of security requirements for healthcare systems, a security DSL is applied to define security requirements during the business process modelling by a business domain expert. Later on these security requirements are refined by a security expert and security enabled application for healthcare is generated.

The healthcare system under study is a SOA environment where services are deployed on different servers at different sites. Each site contains its own database and perform both roles i.e. service provider as well as service consumer. Figure 2 show the abstract architecture of the healthcare system.

Based on the scenario discussed where communication takes places among different healthcare partners having SOA environment, number of security requirements can be identified. Healthcare partners creates, store, send and receive different kind of healthcare documents such as patient’s information, patient’s test results, query result information etc. The scenario presented in Figure 5.1 depicts interaction among two healthcare organizations “Sample Collection Point” and “Medical Test Centers”. Users from these two organizations access resources i.e. services and documents within and from other organization. A patient visits a “Sample Collection Point” and provides his/his demographics and asks for the medical information or any test. The person sitting at the collection point, before interacting with the healthcare system has to prove his/her identity which enables him/her to get an appropriate role in the system and grant him/her permissions based on his/her role. Same is the case with the person sitting in the “Medical Test Center”, when he/she has to interact with the system he/she has to prove his/her identity. The identity validation is performed through authentication mechanism and role/permission verification is performed through Authorization mechanism [34]. The system at the sample collection point and test center validate the person’s credentials representing him/her identity for granting him/her access to the services offered by the sample collection point. These credentials could be username-password or digital certificate etc.

Figure 2. System Architecture of the Healthcare System
In the same context when the “test order” document is sent from sample collection point to test center or “test result” document is sent from test center to sample collection point; users from both places should not be able to deny having participated in the interaction. The security requirement for accountability and auditing is called non-repudiation. Basically it is used for access and usage of resources and if it is ensured then it is not possible for users to deny having accessed the system resources; therefore misuse of medical data can be avoided [34].

Many services are involved in the healthcare system understudy and these are outcome of composition of multiple services with one particular business goal. The dynamic behavior of these services is represented through UML activity diagram [35]. In our work we are focusing only one service Entity Identification Service.

5.4 Entity Identification Service (EIS)

EIS is a HSSP(Healthcare Service Specification Project) specified service which basically focus the patient’s demographics and responsible for the retrieval of patient identification information [36].

![Figure 3. Security annotated Entity Identification Service](image-url)
patient visits the sample collection point and asks for medical information or any test. He/she provides his demographics and his/her record is searched locally. If the record of the patient does not exist on this collection point then the query is send to the external system which may be another collection point or a test center. If patient’s record also does not exist on the external system then a new patient profile is created.

EIS composed of several services whose objective is to identify the patient locally or remotely. The security annotated workflow of the EIS is represented through UML activity diagram and shown in Figure 3.

It is clear from the figure 3, that to access this service, one has to follow proper procedure by “authenticating” himself/herself and if he/she has to perform some action then “authorization” procedure would be followed. When patient information is send to external EIS and when query result is send back to EIS entry point service then “non-repudiation” security requirement would be applied.

5.5 Discussion

SOA applications are basically composition of services which are scattered across the Internet. Web Services are composed using service composition languages/standards which define the execution order of services invocation and their interaction pattern however they do not deal with the early stages of software development. Several web service composition frameworks/methods are proposed, however notion of security is neglected in all of them. Security is not defined during the business process modelling of SOA applications. We have developed a framework for the model-driven development of secure web service composition. In this framework, main steps are same as discussed by different researchers, the main contribution in the MDS service composition framework is incorporating security objectives along the business process modelling, using UML activity diagram. Proposed framework facilitates the business process expert to model the security along the business process modelling for service composition. In the proposed framework, security is defined at two different stages. Firstly at step-1, when the overall modelling of service composition is performed using UML activity diagram. This is the concept building stage about service composition i.e. what functionality this service composition has to perform and which services are required to accomplish this functionality. Secondly at step-3, when all required services are either discovered or developed; now all the required services are available and security will be refine/redefine for modelling service composition using UML activity diagram. This security annotated business process model will be transformed into a service composition using model-driven approach.

5.6 EIS BPEL Workflow Diagram

EIS is composed of many services whose main functionality is to identify a patient locally or remotely. These services are defined in WSDL standard, which is basically a XML format for service definition, containing messages. The operations in WSDL send/receive those messages written in an appropriate message formats. During this work, SOAP message format is used. During this work these business services are just used as they are already developed [35]. A WSDL file is created which contain the method to call the appropriate service. WSDL are known as partner links in BPEL workflow. Web services together with the BPEL constructs make an overall service composition. In this way BPEL act as a container for the web services which are described by their WSDL descriptions.

5.8 System Working

As can be seen from the Figure 4, five business services are involved in the EIS workflow; naming: EIS_EntryPoint Service, Message Generator Service, Parser Service, Database Service and External EIS (XEIS). The EIS session start from the client application which set “Patient_ID” as input information. Security objectives; confidentiality is ensured through authentication security mechanism. After ensuring security; “Patient_ID” information are forward to Message Generator Service, which takes the value and generates the required “Patient Registry Get Identified Query”. The generated message is sent to Parser Service; where it is parsed. The parsed message is then sent to Database Service. The business logic of Database Service consists of Patient Demographic Retrieving Functions.
If the patient record if found locally then it is send to the client application otherwise same request is send to XEIS.

Figure 4: EIS workflow diagram

6. Conclusion

Incorporating security requirement during early stages of software development will improve the security of the Web Information System. A Model Driven security framework is presented for the secure composition of web services where security is modeled along the business process modelling. A business process expert has been facilitated in modelling the security objectives along the business process model for service composition. This security annotated business process model of services composition will facilitate the concrete security implementation. We believe our effort is a contribution towards stressing to incorporate security requirements during early stages of software development i.e. during business process modelling for service composition

7. References


