Enabling Security Requirements for Enterprise Service-Oriented Architecture

Alaeddin Kalantari1, Anahita Esmaeili2, Mojtaba Khezrian3, and Hamed Taherdoost4
1,3,4Faculty of Computer Science and Info System, University Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia
{Alaeddink, Hamed.taherdoost,}@gmail.com, m_khezryan@yahoo.com
2Asan Afzar Sari, Sari, Iran
esmaeili.anahita@gmail.com

Abstract—In today’s Web environment, service-oriented architecture (SOA) becomes as an efficient paradigm to integrate distributed applications. Due to loosely coupled nature of SOA, security is one of the most important items that must be considered in SOA-based environments. Therefore, providing a comprehensive framework to support security in Enterprise SOA (ESOA) recently becomes a critical issue. In this paper logical deployment architecture for ESOA is proposed and then security requirements for the proposed architecture are analyzed. To provide capabilities to meet these requirements, a conceptual security framework which is consists of two approaches namely IBM SOA Security Reference Model and Security Framework for SOA, is presented. Finally, a case study is demonstrated and implemented to show that proposed framework can be applicable for any ESOA.

Index Terms—Service-Oriented Architecture, Enterprise SOA, Logical Security Framework, Logical Deployment Architecture

I. INTRODUCTION

Service Oriented Architecture (SOA) is a collection of services that communicate with each other to fulfill a particular business process. This paradigm passes data between service consumer and service provider either simply or complicatedly. SOA is a popular strategy to provide an integrated, flexible, and cost efficient (Web) Service-based enterprise. It promises interoperability, reusability, loose coupling, and protocol independency of services as core principles of SOA ([1],[2]). Normally, this standard-based approach uses Web Services [3] as building block to support particular business tasks. Web Services are published with Web Services Description Language (WSDL) [4] interface and they use Simple Object Access Protocol (SOAP) [5] as a communication protocol.

Despite the benefit of SOA, integrating applications introduce new security issues and makes security design more complex than before. In the context of SOA, developers must keep services as open and easy to use as possible which can make the applications more vulnerable. In addition, security should not decrease the interoperability of services. Thus, SOA experts must provide the capability to secure the architecture instead of securing a service itself [11]. As a matter of fact, SOA brings several additional security issues. In order to overcome these matters, the various functional and non-functional security requirements are needed to be considered.

Some of these requirements such as authentication, end-to-end security, interoperability, access control, auditing, secure configuration, assurance, and compliance have been presented by [1], [2], and [6]. In addition, some technologies and standards such as XML Signature [7], XML Encryption [8], WS-Security [9], XKMS [10], SAML [11], and XACML [12] have been developed to support the above requirements. However, these techniques and standards cannot provide complete security for ESOA and yet, they are complex and not known enough to SOA developers.

Since location is a focal point of the design of a SOA security solution for ESOA, first a logical deployment architecture is proposed based on three IBM scenarios (Service creation, service connectivity, and interaction and collaboration services) and three kinds of services presented by [1],[2]. Then security requirements for the proposed architecture are analyzed.

Although, a SOA security framework [14] for network-centric environment has been already presented for providing security in ESOA, there are some limitations such as lack of secure configuration, comprehensive audit capability, and adequate infrastructure security. On the other hand, the IBM SOA Security Reference Model [13] has been presented to rectify aforementioned problems. However, this model does not support privacy for all security levels.

To provide capabilities to meet these requirements, a conceptual security framework which is consists of two approaches namely IBM SOA Security Reference Model and Security Framework for SOA, is presented. This security framework can support all layers of Service Oriented Reference Architecture (SORA) [15].

The rest of this paper is organized as follows. Section 2 presents some preliminaries where the security requirements and current references are delineated. In section 3, the IBM SOA Security Reference Model and Network Centric SOA Security Framework are compared. A logical deployment architecture in section 4 is proposed. Section 5 presents the security framework for an ESOA. The proposed framework is tested and implemented using a case study and the result is presented in section 6. Finally, section 7 provides conclusion and future works.
II. PRELIMINARIES

In this section, a brief of security requirements, IBM SOA Security Reference Model, and Network Centric SOA Security Framework is described.

A. ESOA SECURITY REQUIREMENTS

The security requirements of SOA both functional and non-functional must be considered to ensure security in enterprise SOA-based. According to [1], [6], and [13], the following security requirements are identified:

Identity: all entity within an ESOA must be identified. These identities are used for authenticating, authorizing and auditing. An enterprise SOA-based may have various user repositories to address their user’s identity. Thus an appropriate identity provisioning and mapping strategy is required.

Identity repository protection: all repositories that keep users information should be protected.

Trust: establishing the proper trust relationship between the entities in order to avoid signing repeatedly within an enterprise.

Authorization: the authority of an identity should be examined whether this identity is allowed to access the resource.

Authentication: the identity of users must be verified.

End-to-end security: an adequate security solution to protect data from origin to the destination is required.

Interoperability: a standard that can help the services within an enterprise to work with each other without high effort is needed.

Secure configuration: using default security configuration is not enough and an ESOA needs a mechanism to configure additional security features.

Auditing: all events in an enterprise should be recorded as audit information in order to be used for future forensic.

Privacy: protecting sensitive information (e.g. financial information) across a boundary is required

Availability: service consumer must be ensured that required service is available at the right time.

Secure development: developing service in secure manner is vital to ensure security in an ESOA.

Infrastructure security: considering all security required in communication and network levels, intrusion detection, firewall, and physical security are required.

Regulatory compliance: measuring IT systems performance in terms of rules and metrics that defined in policy.

Multi Level Security: providing the capability to process data with different sensitivities and to allow users access to the data with different clearances at different security levels is required.

B. IBM SOA SECURITY REFERENCE MODEL

The IBM SOA Security Reference Model as shown in Figure 1 comes from a set of requirements that are divided into three main layers: Business Security Services, IT Security Services, and Security Policy Management. The Security Enablers Services provide security function for IT Security Services. In this reference model, the Business Security Services layer includes six security solutions such as Compliance and Reporting, Data Protection, Privacy and Disclosure Control, Non-repudiation, Identity and Access, Trust Management, and Secure System and Networks that describe business security requirements.

C. A SECURITY FRAMEWORK FOR SOA

The SOA security framework [14] derives from the security architecture which is based on the Internet protocol stack with two addition layers, the host and the packet as shown in Figure 2, and the Service Oriented Application Layer of NCES [16] which is located within the application layer of the architecture. This framework supports three security levels: content level, communication level, and network level. In sum, it contains of seven layers such as application, transport, host, IP, packet, MAC, and physical layer that are distributed through the three security levels. The application layer of this framework contains of SOA security standards which provide the capability for authentication, access control, policy management, key management, and so on. In this framework privacy encompasses all security levels of networks and is divided into several classes: data privacy, identity privacy, location privacy, existence privacy, transaction privacy, and time privacy. In addition, the availability of the services and systems are ensured on both the content and network levels. In this framework, transport security relies on communication level of security such as SSL/TLS and SSH.
Like privacy, Multi-level security (MLS) covers almost all levels of the architecture. The Management and Access Control encompass all layers and contains various features such as trust management, identity management, and so on. The definitions of other layers have been described in [14].

### III. Comparative Evaluation

In this section, the above references are compared in terms of security requirements that have been explained in section 2.1. These requirements are essential to be considered in order to provide any security framework and model. The comparison result is shown in Table 1. In this table, the Security Framework for SOA has been considered as “SOASF”.

<table>
<thead>
<tr>
<th>Security Requirements</th>
<th>IBM</th>
<th>SOASF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Authorization</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Access control</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>End-to-End security</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Interoperability</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Secure configuration</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Secure Development</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Assurance</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Compliance</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Auditing</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Identity provisioning</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Identity propagation</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Identity management</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Privacy</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Manageability</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Availability</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Trust management</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Policy management</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Key management</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>MLS</td>
<td>N/A</td>
<td>√</td>
</tr>
<tr>
<td>Infrastructure security</td>
<td>√</td>
<td>Low</td>
</tr>
<tr>
<td>Repository protection</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Communication and Network</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

The comparison shows that the security framework for SOA presents all security standard required for the communication and network levels. It relies on the Web Service security standards in order to provide security in the content level. This framework provides the privacy for all security levels and supports Multi Level Security (MLS). The availability of the services and systems is ensured on both the content and network levels. Although, this standard based framework can be used to develop the security in SOA-based environment, there are some limitations that should be considered by developers: First, the framework does not support the secure configuration requirement. Next, this framework does not support the infrastructure security requirements such as physical security, operating system and data base security. Finally, there is no standard for the identity repository protection in this framework.

Unlike the SOA security framework, the IBM SOA Security Reference Model provides capability to support most of security requirements. Regardless of the benefit of this reference, there are still some limitations that developers should take into account: first, this reference model only concedes privacy in content level and provide policy to protect sensitive data such as personal information and financial information. Second, there is no proper mechanism for supporting Multi Level Security (MLS) in this reference model.

### IV. Logical Security Deployment Architecture

Location is significantly important to provide an adequate SOA security solution. In order to provide an appropriate solution that shows exact location of each entity on the real ESOA, designer should find out a proper way to what goes where and takes into account availability requirements, security, and performance. Based on SORA, services can be offered to or from elsewhere and service consumers can be from public, partners, enterprise intranet. According to [1], there are four high level possible locations for ESOA entities: Enterprise, Partners, Managed service provider, Public at large. These locations are not atomic and might be divided into multiple locations. For example an enterprise may be divided into several regions and each region includes datacenters, headquarters, branches, and so on. In most situations, there is a Web services gateway located in the demilitarized zone (DMZ) in front of either a Web application.
server or portal server which enforce identity validation, auditing, authentication, identity, and integrity. In addition, the DMZ may also have the enterprise Web pages and Web Services that are served to outside world either public users or partners. As SORA illustrates, a service can directly access to the existing application or via the intermediaries such as service components. Service can access to the resources via Enterprise Service Bus (ESB). Thus, several connections may need to connect to the resources within the private network. A number of holes are needed for these connections on inner firewall that cause it vulnerable.

In order to rectify this problem, an appropriate service like Service Routing Coordinator (SRC) is proposed to propagate requests for proper resources. SRC is placed in the internal zone and may have two connections. Although, almost all services and servers in the internal zone have a connection with ESB, the relationship between ESB and portal/application server is unilateral. Thus, SRC may connect with ESB and portal/application server. SRC is a content-based router and it also exchanges message format and security token if they are needed. Figure 3 depicts the new logical deployment architecture for an ESOA application including SRC that derives from IBM three scenario (Service creation, service connectivity, and interaction and collaboration services) [13] and three kinds of services presented by [1] and [2]. In this architecture due to the security policies defined between enterprise and partners, the Web Services provided for partners are placed in separate server. In such case, the information format and structure may be different from the Web Services message format provided for the public.

Figure 4 shows the UML sequence diagram of this architecture where a partner sends a SOAP request to Web Service provided for partners. This service must have a connection to the data server.

In the next section, a conceptual security framework which is consists of two approaches namely IBM SOA Security Reference Model and Security Framework for SOA to provide capabilities to meet requirements which are described in section 2, is presented.

V. THE PROPOSED CONCEPTUAL SECURITY FRAMEWORK

As mentioned in section 3, the aforesaid references have been presented for providing security in ESOA. Despite the benefit of these references, there are some restrictions that must be considered. For instance, the SOA Security Framework has no comprehensive audit capability, secure configuration, effective repository protection, and adequate infrastructure security. On the other hand, the IBM SOA Security Reference Model does not support privacy for all security levels take into consideration that multi-level security (MLS) has been overlooked. As shown in Figure 5, in order to overcome above limitations, in this paper an effective conceptual security framework for ESOA is proposed based on [13][14]. This framework can help to address all security requirements that have already been mentioned in this paper and can be applicable to all layers of SORA. The components of this framework derive from the IBM SOA Security Reference Model [14] and the SOA Security Framework for network centric environment [13]. The content level security is divided into three layers; 1) Content Security Services to provide end-to-end message security, 2) Compliance, and Identity and 3) Access Service that provide secure collaboration and interaction. The Infrastructure Security Services includes the communication and network security levels. Privacy and audit encompass almost all three levels. The proposed framework contains the following elements:

A. CONTENT SECURITY SERVICES

These security services are standard-based that provide end-to-end message level security. It consists of two services: Confidentiality Service encrypts and decrypts documents and protects information from disclosure. Integrity Service provides the capability to sign document in order to protect information against unauthorized modification.

In this part, WS-Security specification provides end-to-end message security which is independent from the transport layer protocol (e.g. SSL). In addition, XML-Encryption, XML-Signature, and PKI can be used to assure the document security.
Identity and Access Services are various consistent components/services that provide the capability for managing, sharing, federating, and accessing identity information from a set of identity repositories. These set of services must be flexible, reusable, standard-based, and configurable which can be used by different components of SOA environment such as service consumer and provider, proxy servers, portal servers, application servers, and data servers. The definitions of these services are explained as following:

Identity and Access Services optimize user interaction by managing identities both within and across boundaries, and include provisioning and de-provisioning identities and self-care/self-registration. In addition, Identity and Access services provide the capability to manage identity life-cycle and user password, and include policies that allows identity access to the IT resources.

Identity Foundation Services provide a technology to synchronize user repositories and manage, store, and use the organization entities information such as users, group, and roles in order to mange identities relationship and secure access to their information.

Identity Provisioning Services provide the policy-based paradigm for creating, managing, and deleting the accounts across the appropriate identity repositories. Identity Provisioning provides user self-service and password synchronization capabilities as well as automated approach to manage the user password. Standard–based federated provisioning such as SPML and WS-provisioning can be used to enable collaboration between different technologies [13].

Identity Propagation Services provide capabilities for mapping and exchanging trusted identity in order to propagate them across the boundaries.

Authentication Services provide capability to support multiple authentication mechanisms and validate identities. These services can be created on open standards and technologies such as WS-Trust, Kerberos, Security Assertion Markup Language (SAML), and Public Key Infrastructure (PKI) in order to provide interoperability. The security token service (STS) can be used for this capability.

Authorization Services provide capabilities to decide whether an identity is allowed to access a resource. In order to make a decision, policies are enforced by Policy Enforcement Point (PEP) that depends upon decision made by a Policy Decision Point (PDP). Authorization Service has two key points for decision: Authorization Policy and Authenticated User.

Non-Repudiation Services provide capabilities to ensure that sender and recipient cannot falsely deny that they didn’t send or receive data.

Availability Services provide a response to a request in a timely manner. Ensuring that services are available when required is a key in many SOA environments. These services ensure two types of availability; Network resource availability and Service availability. The availability can be ensured in network layer that can be performed with Communication and Network Service by deploying the Packet Level Authentication (PLA). Architecting for high availability includes application clustering, database clusters, and similar techniques.

D. Infrastructure Security Services

Infrastructure Security Services provide capabilities to support communication and network levels security, operating system, database and front-end security. They also provide physical security in each layer of reference architecture. The definition of each service is explained in detail as following:

Communication and Network Level Security Services are concerned with all security aspect related to communication and network levels of security architecture. Indeed, this services use link encryption and authentication on the MAC layer and on the Packet Layer use Packet Level Authentication (PLA). In some cases, IPsec is used to provide security in network level and communication level. On the host layer, security is provided by Host Identity Protocol (HIP) architecture. In addition, the transport layer provides point-to-point security using TLS/SSL and SSH protocol.

Operating System and Database Services provide capabilities to protect operating system against unauthorized access and threats. Moreover, it provides database security, Virus detection, and host based intrusion detection.

Front-end Services protect applications and data against malicious inputs and threats. These services provide input validation, output encoding, secure session handling, secure data replication.
**System Security Services** are technologies to protect infrastructure servers, systems, and networks against security threats. For instance, providing firewalls and proxies, intrusion detection, physical security systems.

**E. Privacy Services**

Privacy Services protect sensitive information across all security levels. This service defines policies to classify sensitively of information for use in transit and at rest. These services support data privacy, identity privacy, location privacy, existence privacy, transaction privacy, and time privacy [14]. They can be accomplished through middleware, data encryption, hardware, and operation system (OS) [13]. This externalization can help to manage data protection. Privacy Services are usually created into other security services, such as encryption schemes, network design, cryptographic key management, network utilization, and so on. They have strongly relationship with Audit Services because when the sensitive data are acquired, Audit Services must record those events in detail.

**F. Audit Services**

Audit Services provide mechanisms to collect, store, and submit every events across business systems based on standards like common base event (CBE) [21]. Centralization of audit can help to provide the capability for investigating of events in future.

**G. Trust Management Services**

Trust Management Services provide multiple trusted relationships (e.g., business-to-business [B2B] and system-to-system [S2S]) between various entities such as organization, enterprise, security domains. In fact, Policy-based and reputation-based are two approaches for managing trust in SOA boundaries.

**H. Multi Level Security (MLS)**

Multi Level Security provides the capability to process data with different security clearances in the SOA environment.

**I. Security Policy Management Services**

Security Policy Management Services provide mechanisms to define, manage, monitor, and enforce security policies throughout the business process for authenticating and authorizing entities, auditing events, and protecting information. A proper trust model can be used to propagate security context across business systems. Thus, these services are focal points of providing appropriate security capabilities in an ESOA. These services provide policies with common formats such as WS-Policy and XACML.

**J. Governance and Risk Management**

Governance and Risk Management framework provides the mechanism that individuals can control the SOA system efficiently. This framework provides the capability to implement and enforce security policies within the boundary.

**VI. Case study**

Razavi Financial Institute (RFI) is a banking based firm of approximately 20,000 customers and 5 small branches in different locations that provides multiple services for its customers. Recently, this institute acquired a small insurance company of approximately 5000 customers that is called Maz Salamat Insurance Company (MSIC). Each customer formerly from MSIC has a user identity in the RFI portal. RFI wants to be able to reuse the business logic in MSIC applications to offer new products to its customers and it is expected that these applications can be reused in other parts of the RFI business. Currently, RFI has added a link to connect to the MSIC portal for whose have already been the customers of MSIC. The problem is the customers have to memorize two usernames and Passwords for both systems, RFI and MSIC. Recently, the number of RFI customers is growing up to 1000 customers in month. The team managers decided to achieve new system to provide the capability to add new services in order to entice new and current customers. In addition, RFI plans to offer the functionality of its application as web services to its partners. Moreover, it plans to buy more companies related to its business activities in future. Its managers expect that new system be flexible to change and connect to other system applications. Furthermore, they wanted to use current systems and applications due to cost limitation.

The deployment architecture of this case study has been designed using the proposed logical deployment architecture and then the proposed conceptual security framework has been applied to provide an appropriate security solution for this case study. In this case study, the SRC service has been implemented to decrease the number of holes in the inner firewall. In addition, the web service for partner server has been located in DMZ behind the inbound Web services security gateway. WSO2 Web Services Framework/PHP (WSO2 WSF/PHP) have been used for implementing this case study services.

In the process of this case study, customer sends the username and password via web browser; in such case, the transfer security protocol such as SSL/STL can be used to protect the user identity information against unauthorized person. This service is a simple form that is designed with HTML. Further, a Web Service Client is implemented to provide end-to-end security with encrypting and signing the message. This file is named as client_web.php and is placed in project2 directory as depicted in Figure 6.

Once the inbound web services gateway receives the respond from the authentication service, it should make decision for sending authenticated identity to the SRC. The SRC send authenticated identity with exchanged request to the portal. The portal provides a Web page for costumer to choose a service. Then, portal sends authenticated identity to authorization service in order to examine whether the customer has authority to access the resource. If so, portal generates a SOAP message and sends to the selected service
with authenticated identity. In this case the identity information for RFI is equal with the identity for the portal, thus no need to mapping and invoking STS Service. Figure 7 shows portal main page that allows the customer choose a service. More details regarding implementation of this case study can be seen in [22].

CONCLUSION AND FUTURE WORK

In this paper, a logical deployment architecture for ESOA including a Service Routing Coordinator (SRC) to propagate requests for proper resources is proposed. Moreover, a conceptual security framework for enterprise service oriented architecture, as a part of ongoing research, is proposed. In that case, security requirements for the proposed architecture are identified and the IBM SOA Security Reference Model and Security Framework for SOA are compared. Thus, in order to provide capabilities that alleviates those limitations that shown in the result of comparison, these approaches are combined to provide a new security framework. The proposed framework supports all three security levels similar to SOA Security Framework, privacy, and MLS. The framework is applicable to all layers of Service Oriented Reference Architecture (SORA). The result of demonstrating and implementing a case study shows that the framework can be applicable for any ESOA. The implementation of all defined services in the framework can be considered as future works of this research.

REFERENCES