International Journal of Advanced Computer Science and Information Technology (IJACSIT)
Vol. 1, No.1, October 2012, Page: 25-31, ISSN: 2296-1739

www.elvedit.com

A Service Oriented Security Reference Architecture

Authors

Alaeddin Kalantari *alaeddink@gmail.com*
Faculty of Computer Science and Information System, Universiti Teknologi Malaysia (UTM) *Kuala Lumpur, Malaysia*

Anahita Esmaeili *esmaeili.anahita@gmail.com*
IT department, Asan Afzar Sari *Sari, Mazandaran, Iran*

Suhaimi Ibrahim *suhaimiibrahim@utm.my*
Faculty of Computer Science and Info System, Universiti Teknologi Malaysia (UTM) *Kuala Lumpur, Malaysia*

Abstract

Nowadays, service-oriented architecture (SOA) is used as an efficient solution to integrate distributed applications in an enterprise. In a SOA-based environment, security is one of the most important issues that must be considered on account of loosely coupled nature of SOA. However, there are several approaches and technologies for securing services such as WS-Security, SAML, and etc. SOA brings additional security problems on the level of architecture. Therefore, providing comprehensive security reference architecture for Enterprise SOA (ESOA) becomes a critical issue. In this paper, we propose a Service Oriented Security Reference Architecture (SOSRA) for Service Oriented Reference Architecture (S3) based enterprise applying our previously proposed Conceptual SOA Security Framework.

Key Words

Service Oriented architecture, SOA, SOA Security, SOA Security Framework.

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 as building block to support particular business tasks. Web Services are published with Web Services Description Language (WSDL) interface and they use Simple Object Access Protocol (SOAP) 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 [1].

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 [4]. 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.

To provide capabilities to meet security requirements, in our previous paper [4] we have proposed a conceptual security framework which is consists of two approaches namely IBM SOA Security Reference Model and Security Framework for SOA [14]. This security framework can support all layers of Service Oriented Reference Architecture (SORA) [14]. In this paper we propose a Service Oriented Security Reference Architecture (SOSRA) for Enterprise which is designed based on Service Oriented Reference Architecture (S3) using our previously proposed Conceptual SOA Security Framework [4].

The rest of this paper is organized as follows. Section 2 presents some preliminaries such as web services, Service Oriented Architecture (SOA), Service Oriented Reference Architecture (S3), and A Conceptual Security Framework for ESOA. In section 3, the Service Oriented Security Reference Architecture (SOSRA) is proposed. Finally, section 4 provides conclusion and future works.

II. PRELIMINARIES

In this section, a brief of Web Services, Service Oriented Architecture (SOA), Service Oriented Reference Architecture (S3), and A Conceptual Security Framework for ESOA is described.

A. Web Services

According to [3], Web Services are loosely coupled computing services that can reduce the complexity of building business applications, save costs, and enable new business models. Web Services are application components that using open protocols to communicate and they are self-contained and self describing. Web Service can be discovered using UDDI and used by other applications. Extensible Markup Language (XML) is the basic for Web Services. Web Services can be able to publish the functions and data to the rest of the world.

Another definition of Web Service is provided by IBM [4], A Web Service is a software interface that describes a collection of operations that can be accessed over the network through standardized XML messaging. It uses protocols based on the XML language to describe an operation to execute or data to exchange with another Web Service.

B. Service Oriented Architecture (SOA)

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 as building block to support particular business tasks. Web Services are published with Web Services Description Language (WSDL) interface and they use Simple Object Access Protocol (SOAP) as a communication protocol. Figure 1 shows the operation that each component can perform.

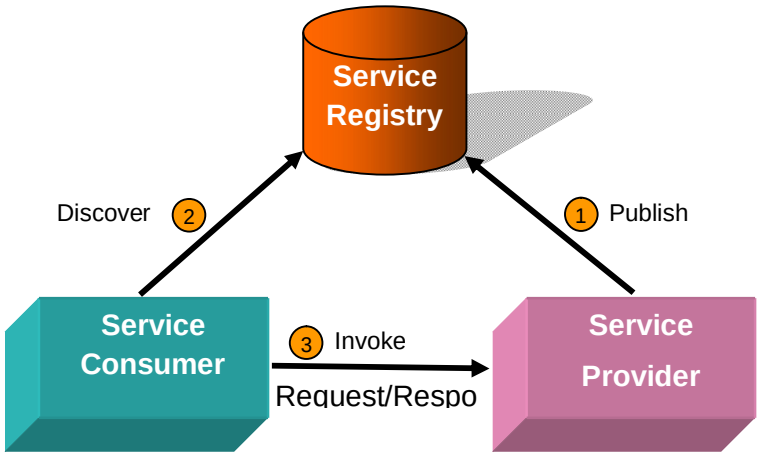

FIGURE 1: SOA COMPONENTS AND OPERATIONS.

C. S3: Service Oriented Reference Architecture (SORA)

In order to design an architectural framework with interconnected architectures, transformation capabilities and reusability IBM presented Service Oriented Reference Architecture (S3) [14] which is a high-level SOA model that shows the conceptual building blocks of an SOA solution, and the relationship between them. Each layer represent different business value perspective and they are significantly separate business. S3 can be used as a basis for specific solution models, and also for models of larger SOA systems such as ESOA. The architect can easily create an SOA in concert with methods such as Service- Oriented Modeling and Architecture (SOMA)[14].

Each layer has a logical and physical aspect. The logical aspect includes all the architectural building blocks, design decisions, options, and key performance indicators and so on while the physical aspect covers the realization of each logical aspect using technology and products. This section will focus on logical aspect of the S3.

As shown in Figure 2, the first five layers contain building blocks whose purposes relate to business functionality. They support each other in a hierarchy, although its layering is not strict. The rest of layers support the layers related to business functionality, but do not support each other in a strictly layered hierarchy

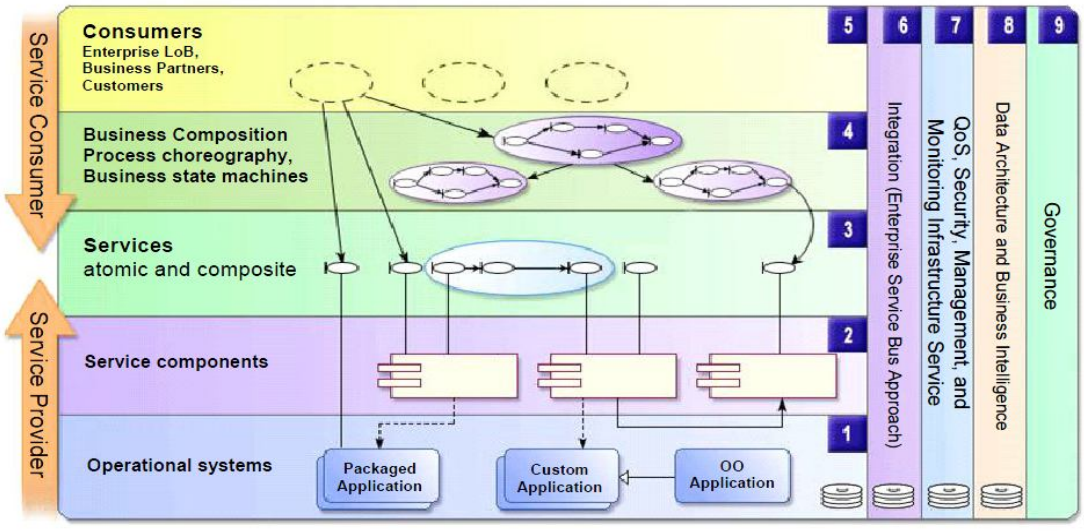

FIGURE 2: S3: SERVICE ORIENTED REFERENCE ARCHITECTURE.

D. SOA Security Framework

This framework can help to address all security requirements that have already been mentioned on [4] and can be applicable to all layers of SORA. The components of this framework derive from the IBM SOA Security Reference Model [13] and the SOA Security Framework for network centric environment [14]. 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.

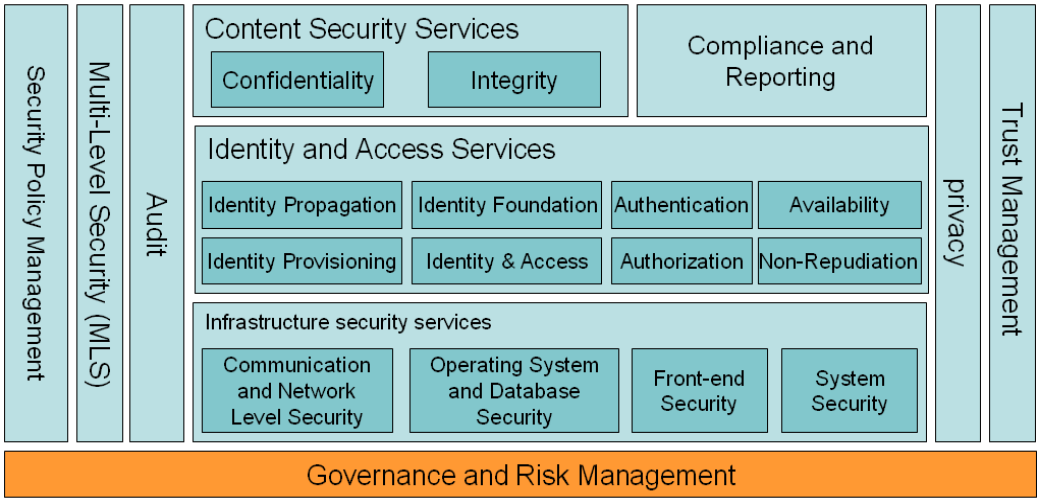

FIGURE 3: SOA SECURITY FRAMEWORK.

III. SERVICE ORIENTED SECURITY REFERENCE ARCHITECTURE

Service Oriented Reference Architecture (s3) can be used as a basis for specific solution models, and also for models of larger SOA systems such as ESOA.

As Figure 2 shows from up to down approach, service consumers can provide requests for services directly or alternatively. They start a business process that called service. Services are described with service definition. Service components are used as intermediaries to expose existing application functions for those applications that cannot be directly exposed.

The Conceptual Security Framework can be applied on Service Oriented Reference Architecture (S3) in order to insure security for each layer. Client is authenticated at the consumer layer as defined identity. The customer layer determines if the user is authorized to access the service layer or business layer. If so, the request and identity are propagated to service provider. All events should be registered as Audit information to verifying performance of consumer layer according to the policy. This information should be stored in audit storage and must be applied for all layers. Trust service is needed to establish trust relationship between layers to avoid sign in repeatedly.

All messages during transformation should be protected and confidentiality, integrity, and privacy of message should be assured. The availability of the service must be assured. Service consumer and business process layer should be able to access to the correct service in an exact time. The federated identity provisioning and appropriate identity integrator are required for all layers. Security infrastructure encompasses almost all layers. Security infrastructure is

concerned with all aspect of security development, communication and network security, firewall, intrusion detection, and physical security.

Operation layer is the last layer of S3 nine-layers where consumer goals to access the application functions to perform its needs. There is no resource or layer after operation layer that the applications in this layer want to access it. Thus, there is no reason to map identities in this layer even if the applications have communication with each other. For instance, the existing application may need to connect to the data server but their relationship is defined based on traditional approach.

According to the security framework and security requirements for Service Oriented Reference Model (S3), a new Service Oriented Security Reference Architecture (SOSRA) is proposed. In order to get a good grasp of this architecture a 3D architecture as shown in Figure IV is designed. The first six main layers (consumer, business process, service, service component, operational, and ESB layer) are placed in top of this architecture and then the relevant security services for those layers are designed respectively.

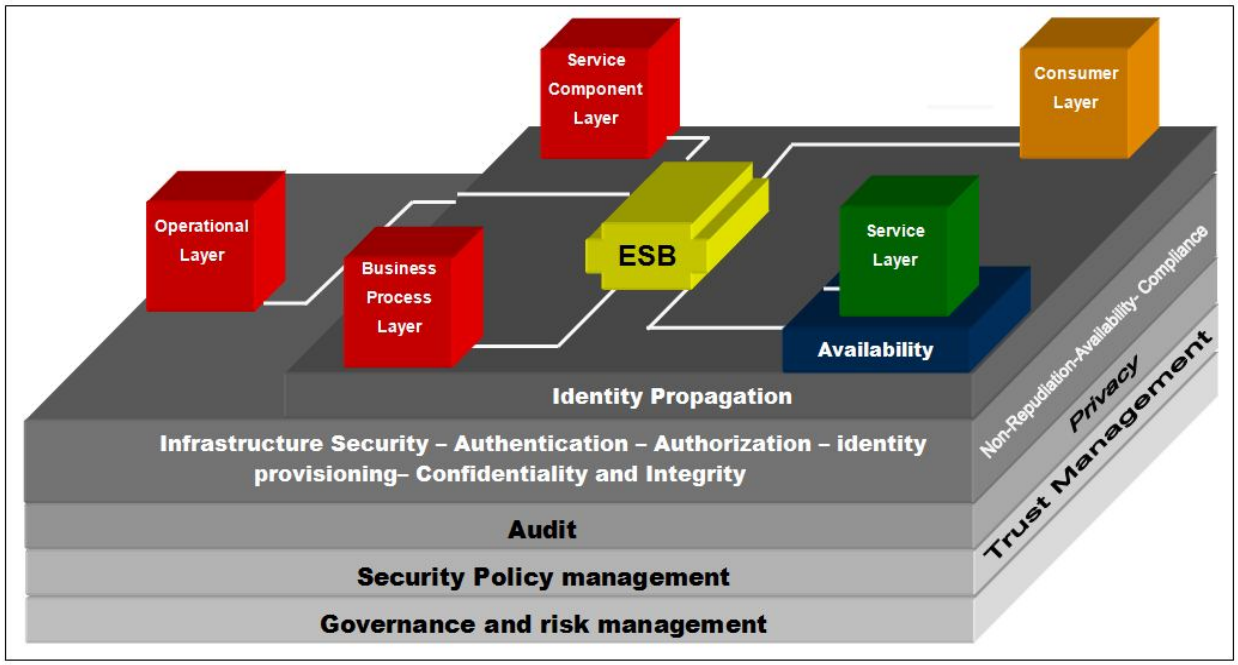

FIGURE 4: PROPOSED SERVICE ORIENTED SECURITY REFERENCE ARCHITECTURE(SOSRA).

IV. CONCLUSION

In this paper, a brief description of conceptual security framework for enterprise service oriented architecture is provided. In addition to that, we have explained S3: Service Oriented Reference Architecture (SORA) and its layers. Then, we applied the security framework for ESOA on SORA to provide comprehensive and high level security reference architecture. Finally, A Service Oriented Security Reference Architecture (SOSRA), as a part of ongoing research, is proposed. The detailed functionality and component of each part of this high level architecture

can be considered as future works. We will also need to validate whether the new architecture is compatible with our logical deployment architecture proposed on our previous paper.

ACKNOWLEDGMENT

This research is supported by Ministry of Higher Education (MOHE) Malaysia and Universiti Teknology Malaysia (UTM) and IT department of Asan Afzar Sari Company.

REFERENCES

[1] Ramarao,k. & Prasad, C.(2008). *SOA Security*. USA: Manning Publication.

[2] Eric Pulier & Hugh Taylor. (2006). *Understanding Enterprise SOA*. USA: Manning Publication.

[3] Web Service Activity, http://www.w3.org/2002/ws/

[4] Kalantari, A., Khezrian, M., Esmaeili, A. and Taherdoost, H. (2011). Enabling Security Requiremets for enterprise Service Oriented Architecture. *International Journal of Recent Trends in Engineering and Technology*, The Association of Copmuter Electronics and Electrical Engineers (ACEEE), 6(1), 75-81 .

[5] New to SOA and Web Service, http://www.ibm.com/developerworks/ webservices/newto/service.html

[6] M. Schumacher, D. Witte. (2007). Secure Enterprise SOA: known and new security challenge, Datenschutz und Datensicherheit.

[7] XML- Signature. (2001). Retrieved 2009, from W3C: http://www.w3.org/Signature/

[8] XML-Encryption. (2002). Retrieved 2009, from W3C: http://www.w3.org/Encryption/

[9] S. Thompson. (2003, 04 01). Implementing WS-Security. Retrieved 2011, from IBM: http://www.ibm.com/ developerworks/webservices/library/ws-security.htm

[10] W. Ford. (2001, 03 30). XML Key Management Specification (XKMS). From W3C: http://www.w3.org /TR/xkms/

[11] Security Assertion Markup Language (SAML). From OASIS: http://docs.oasis-open.org/security/saml/v2.0/

[12] eXtensible Access Control Markup Language (XACML). From OASIS: http://www.oasis-open.org/committees/ tc_home.php?wg_abbrev=xacml

[13] A. Buecker et al. (2007). *Understanding SOA Security: Design and implementation*. USA: IBM Publication.

[14] C. Candolin. (2007). *A Security Framework for Service Oriented Architectures*. Military Communications Conference, 29-31 Oct. MILCOM 2007: IEEE.

[15] Arsanjani, A.(2007). S3: A Service-Oriented Reference Architecture. *IEE Computer Society*, 9(3), 10-17.