SA4WSs: A Security Architecture for Web Services

Lingxia Liu[1,2,3], Dongxia Wang[1,2], Jinjing Zhao[1,2], and Minhuan Huang[1,2]

[1] Beijing Institute of System Engineering, Beijing, China
[2] National Key Laboratory of Science and Technology on Information System Security, Beijing, China
[3] The Information and Navigation Institute, Air Force Engineering University, Xi'an, China
lingxia_liu@tom.com, dongxiawang@126.com, misszhaojinjing@hotmail.com, huangmh06@mails.tsinghua.edu.cn

Abstract. With the rapid development and wide application of the Web services, its security flaws and vulnerabilities are increasing. Security has become one of the key issues to constrain the development of Web services technology. In this paper, we focus on how to build a security architecture for Web services to meet the security requirements of Web service applications. On the basis of analyzing the existing methods, a new security implementation approach for Web services is proposed to meet both the common security requirements of Web services platform and the specific security requirements of Web service applications. Then a security architecture for Web services is proposed. The architecture supports separating the functional implementations of Web service from the non-functional implementation of Web service, and ensures the portability of the platform.

Keywords: Web service, Security, Architecture.

1 Introduction

As a new Web application model, Web service is heterogeneous, dynamic and loose coupling, and introduces a great deal of special threats to Web service applications, and makes that traditional security techniques are inadequate to solve the security issues in Web services.

In recent years, many research institutions, organizations and companies devote to the research of security for Web Services. Organizations and research institutions for Standardization mainly concern in security standards for Web service. The academic community tries to solve the security issues from the theoretical aspect. Middleware companies and open source organizations try to provide security protection tools for customers by providing a set of software or toolkit.

In the paper, we focus on how to build security architecture for Web services to meet the security requirements of Web service applications. On the basis of the improved approach, a security architecture for Web services named SA4WSs (Security Architecture for Web Services) is proposed. The architecture supports separating function implementation of service from non-functional implementation of service, meanwhile ensure the portability of the platform.

K. Mustofa et al. (Eds.): ICT-EurAsia 2013, LNCS 7804, pp. 306–311, 2013.
IFIP International Federation for Information Processing 2013

The remainder of this paper is organized as follows. In section 2, the related works are reviewed. In section 3, the security architecture for Web services is set forth. Finally, in Section 4, we conclude the paper.

2 Related Works

Many Organizations for Standardization, research institutions and companies research on the security architecture for Web services.

2.1 Security Standards

In order to assure the end-to-end security for SOAP message and improve the interoperability of Web service, OASIS and other organizations define the Web Service Security model consisting of multiple standards [1]. The model is insufficient. It is only to protect the two trust sides to communication by a secure connection, and not address the security problem caused by anonymous consumers invoking Web service or SOAP API.

W3C proposed a standard named XML Signature Syntax and Processing specification, which defines how to sign part or all of one XML document [2]. W3C also proposed a standard named XML Encryption Syntax and Processing, which defines how to encrypt part or all of one XML document [3].

2.2 Security Architecture

U.S. DISA (Defense Information Systems Agency) released a specification named "Network Centric Enterprise Services security architecture (version 0.3)" in 2004, provides a service-oriented information security reference architecture to ensure the security of services in network-centric environment [4].

IBM proposes the service-oriented security reference modeling and architecture based on its own SOA infrastructure and business scenarios to cope with information security issues for work flows [5]. The service-oriented security architecture proposed by IBM is meaningful, but its portability is restricted because it relies heavily on its own SOA technologies and products.

GSI provides basic security services for grid computing environments. It is an integrated solution to solve the security issues in grid computing and becomes a standard of GGF [6]. The major security functions in GSI include Certificates, Mutual Authentication, Confidential Communication, Securing Private Keys, and Delegation and Single Sign-On. GSI also has some disadvantages, such as frequent, complex and poor scalable authentication between entities.

OGSA is proposed by Ian Foster et al. on the basis of five-level hourglass structure and Web services [7]. A basic premise of OGSA is that everything is represented by a service, not excepting security. All kinds of security mechanisms such as encryption, access control, and audit are represented as services to facilitate the implementation of the security-related policies.

The service oriented security architecture named SOSIE presented by [8] is realizing the security functions into modular, stand-alone security services. The article [9] addresses the question of security mechanisms that are usually used and that can be used in Web services based SOA implementation from standardized as well as technical and implementation point of view, and gives an overview of SOA security solutions. The article [10] provides a set of software architecture viewpoints that allow security architects to construct a holistic system design based on a set of views. Other related works focus on the special issues of security service [11] [12] [13].

2.3 Supporting Platform

In addition, some research institutions and companies have also developed multiple security platforms and middlewares for Web service.

Microsoft proposed a solution for Web services security problems named WSE (Web Services Enhancements) on the basis of .NET platform [14]. WSE is a service security middleware for .NET platform, including authentication and encryption library. It allows developers to develop secure Web service by implementing the latest WS-Security specification.

Globus Toolkit is the reference implementation of OGSI. It provides basic security services required by grid computing, including message protection, authentication, authorization, and audit/log [15].

The Apache WSS4J project provides a Java implementation of the primary security standard for Web Services, namely WS-Security [16]. WSS4J ships with handlers that can be used in Axis-based web services for an easy integration.

3 Security Architecture for Web Services

3.1 Improved Security Implementation Approach

Web service applications face threats including the threats the Web services platform faced where service located and the threats the service implementation faced, i.e. common threats the platform faced and specific threats the application faced. The first approach [8] can cope with specific threats the application faced, but cannot cope with the common threats the platform faced. The second and the third approaches can cope with the common threats the platform faced, but cannot cope with the specific threats the application faced.

We try to improve the three approaches to meet the security requirements of Web service applications. The first approach cannot cope with a lot of attacks (such as SOAP message replay attacks) the platform faced, no matter how to transform it, because the communication between service implementation and resource gateway is no longer via SOAP message. The third approach is similar to the firewall, and it is not suitable to add application-specific security mechanisms to cope with specific threats the application faced.

Therefore, we focus on improving the second approach to cope with both common threats the platform faced and specific threats the application faced. Analysis on the

Web services platform showed that the platform can be logically divided into two parts. One part of it is Web services runtime environment, mainly providing the functions including deployment, management, publishing and finding for Web service. The other part is resource gateway, which are a set of interfaces between Web services runtime environment and service implementation. It provides the protocol conversion functions for specific application-related invoking. In view of the above analysis, an improved security implementation approach is proposed, as shown in Figure 1.

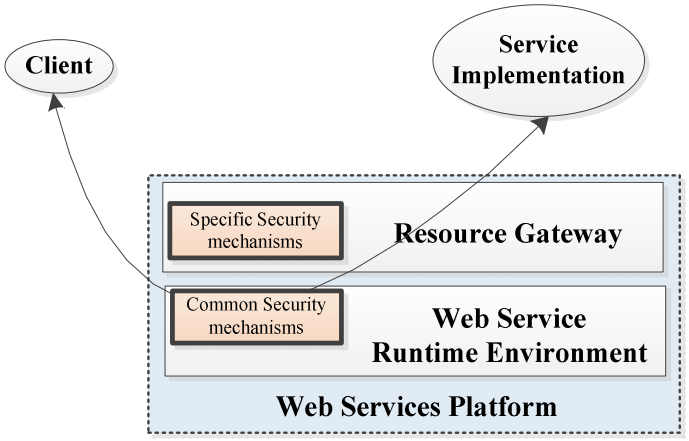

Fig. 1. The improved security implementation approach

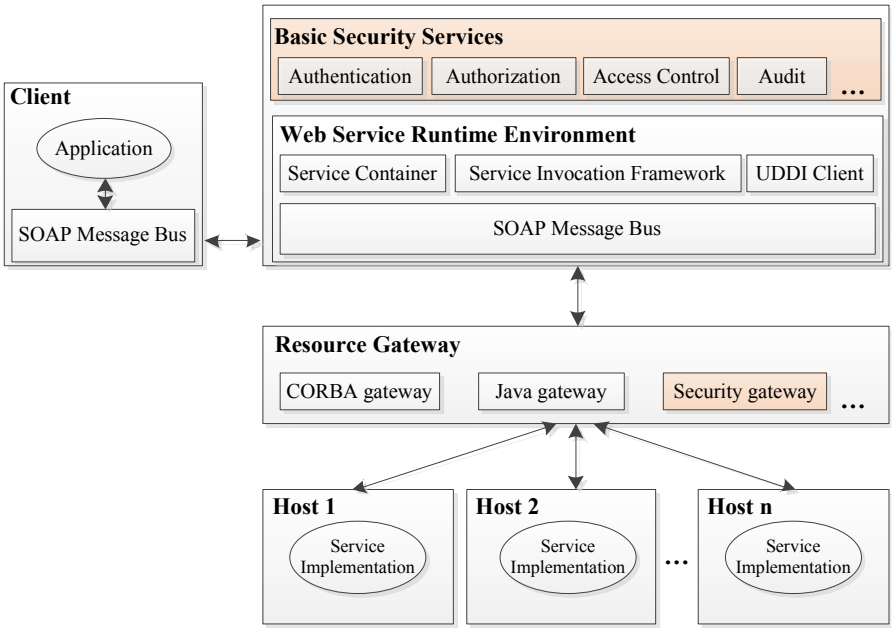

Fig. 2. Security architecture for Web services

In this approach, the security mechanisms are divided into two parts. One part of it is common security mechanisms, which is not relevant to applications and resides in the Web services runtime environment. The other part is specific security mechanisms, which is relevant to applications and resides in the resource gateway. The improved approach not only remains separating functional implementation from non-functional implementation, but also assures the portability of the platform.

3.2 Architecture

A security architecture for Web services named SA4WSs is proposed, as shown in Figure 2.

In the architecture, the module of Basic Security Services provides basic services for implementing the basic security functions, including authentication, authorization, access control and audit, etc. [8]. The module of Security gateway is responsible for the application-specific security functions, and the service implementation is responsible for the business logic. The Security gateway interacts with the service implementation via various protocols (The protocol type is decided by the type of service implementation).

4 Conclusion

In this paper, a security architecture for Web services is proposed. The architecture described in the paper supports separating the functional implementations from the non-functional implementation, and ensures the portability of the platform. SA4WSs has been partially implemented based on Apache Axis. Future work consists of implementing a Web Services security supporting platform to support the development and management of security Web service.

Acknowledgements. This research is supported by National Natural Science Foundation of China (Grant No. 61100223 and No. 61271252).

References

1. Gerié, S., Hutinski, Ž.: Standard Based Service-Oriented Security. In: 18th International Conference on Information and Intelligent Systems, pp. 327–335. IEEE Press, Croatia (2007)
2. W3C: XML Signature Syntax and Processing Version 2.0. Standard, W3C (2012)
3. W3C: XML Encryption Syntax and Processing Version 1.1. Standard, W3C (2012)
4. Defense Information Systems Agency. A Security Architecture for Net-Centric Enterprise Services (NCES) Version 0.3. Technical report, Defense Information Systems Agency (2004)
5. Buecker, A., Ashley, P., Borrett, M., Lu, M., Muppidi, S., Readshaw, N.: Understanding SOA Security Design and Implementation. Redbook, IBM (2007)

6. Overview of the Grid Security Infrastructure, http://www.globus.org/security/overview.html
7. Foster, I., Kishimoto, H., Savva, A.: The Open Grid Services Architecture, Version 1.5. Technical report, Global Grid Forum (2006)
8. Opincaru, C., Gheorghe, G.: Service Oriented Security Architecture. Enterprise Modelling and Information Systems Architectures 4(1), 39–48 (2009)
9. Gerić, S.: Security of Web Services based Service-oriented Architectures. In: MIPRO 2010, pp. 1250–1255. IEEE Press, Croatia (2010)
10. Peterson, G.: Service Oriented Security Architecture. Information Security Bulletin. 10, 325–330 (2005)
11. Lee, S.M., Kim, D.S., Park, J.S.: A Survey and Taxonomy of Lightweight Intrusion Detection Systems. Journal of Internet Services and Information Security 2(1/2) (February 2012)
12. Hori, Y., Claycomb, W., Yim, K.: Guest Editorial: Frontiers in Insider Threats and Data Leakage Prevention. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, JoWUA 3(1/2) (March 2012)
13. Ho, S.M., Lee, H.: A Thief among Us: The Use of Finite-State Machines to Dissect Insider Threat in Cloud Communications. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, JoWUA 3(1/2) (March 2012)
14. Web Service Enhancement 3.0, http://msdn.microsoft.com/en-us/library/bb896679.aspx
15. The Globus Alliance, http://www.globus.org/toolkit
16. Apache WSS4J, http://ws.apache.org/wss4j/