Design of New Architecture for Providing Secure Web Services

E.Uma, A.Kannan, R. Ramesh

Abstract: The main objective of this paper is to improve the end-to-end security properties of information flow in web-based applications which requires simple end-point software and extensions to existing security protocols. Web Service Platform(WSP) and ISO-WSP often perform all Web-service-related processing including security-sensitive information in the same protection domain, so the entire WSP may have access to security-sensitive information. To address this problem, an attempt is being made to develop a new architecture that decomposes the current WSPs into three parts executing in the separate protection domain.

KeyWords: Web Service Platform, ISO-WSP, Web service security

I. INTRODUCTION

Web-based applications and services are increasingly being used in security-sensitive tasks. Current security protocols rely on two crucial assumptions to protect the Confidentiality and integrity of information: First, they assume that end-point software used to handle security-sensitive information is free from vulnerabilities. Secondly, these protocols assume point-to-point communication between a client and a service provider. However, these assumptions do not hold true with large and complex vulnerable end point software such as the Internet browser or web services middleware or in web service compositions where there can be multiple value-adding service providers interposed between a client and the original service provider.

To address the problem of large and complex end-point software, it is proposed to develop architecture which splits existing software into three parts: a highly trusted part that handles security-sensitive information and a legacy, untrusted part that handles nonsensitive information without access to sensitive information, and medium-trusted part that handles the information between theses two stages. The proposed architecture greatly reduces the size and complexity of the trusted code, thereby making exhaustive testing or formal analysis more feasible.

Manuscript received April, 2011, revised August 10, 2011.

E.Uma is Research scholar and Assistant Professor with the Department of Information Science and Technology, Anna University Chennai, Chennai 600 025. (e-mail: euma@annaumiv.edu).

Professor Dr.A.Kannan is with the Department of Information Science and Technology, Anna University Chennai, Chennai 600 025.

Dr.R.Ramesh is with the Department of Electrical and Electronics Engineering, Anna University Chennai, Chennai 600 025. (e-mail: rramesh@annauniv.edu).

II. STUDY OF RECENT TRENDS IN WEB SERVICE SECURITY

Nils[1] provided an overview of current security standards for XML and Web services and also discussed standards include XML Signature, XML Encryption, the XML Key Management Specification (XKMS), WS-Security, WS-Trust, WS-SecureConversation, Web Services Policy, WS SecurityPolicy, the eXtensible Access Control Markup Language (XACML), and the Security Assertion Markup Language (SAML). Jinpeng et.al.[2] have presented ISO-WSP, a secure information flow architecture, to counter the problem of large and complex WSPs [2]. Carsten Rudolph et.al [3] identified the specific security requirements for distributed workflows and provided a decentralized workflow execution mechanism. They ensured that each web service can access only the information which is needed for the correct execution of the invoked operations. Nuno Antunes and Marco Vieira [4] presented an experimental study on the comparison of several web vulnerability detection tools and the results shows that web services programmers should be very careful when selecting a vulnerability detection approach.Shenghui Zhao et.al [5] defined a trustworthy Web Service, and presented a framework for managing Web Service’s trustworthiness. The definition of trustworthy Web Service is integrated availability, reliability, response time, as well as reputation and security. Elias Pimenidis and Christos K. Geogiadis [6] explained to address the issues of security requirements and evaluation criteria [6].

The various security attacks in web service has been discussed and the attacks were categorized into to three main groups as XML Injection, Denial of Service (DoS) and Counterfeit XML Fragment[7]. A Web Service is an emerging technology used to enable applications to communicate more effectively and efficiently because of its interoperability that seamlessly allow various connectivity. Though it seems an advantage using Web Services in a business organization, the security risks that it poses must be analyzed [8]. WS-Security is a framework for providing quality of protection to SOAP messages. WS-Security provides mechanisms for ensuring message integrity, confidentiality and authenticity. Web Services Trust Language (WS-Trust) [10] is an extension to WS-Security that provides means to establish trust relationships amongst differing trust domains. Other frameworks such as WS-SecureConversation and WSSecurityPolicy aim to build on top of WS-Security and WS-Trust to provide other features such as establishment of a secret context or specify policy assertions.

Marzouk.S.Mokbel and Le Jiajin[11] presented several points of the main pivots of the web services security architecture, security challenges and described a number of important emerging standards in field . The focus of this paper is propose the main challenges for securing Web Services and summarizes emerging standards of web services security mechanisms. Artem et.al.[12] described some of WS security threats as well as security attack ontology and explain ed how they relate to each other [12] and also they developed the security attack ontology for WS and illustrated the benefits of using it with an example. Security protocols such as SSL, TLS, https and WS-Security [13] have been developed to protect the confidentiality and integrity of sensitive information in web-based applications. These protocols protect data flow from the client machine to the server machine and vice versa, in the process assuming that the client and server software are trustworthy. The security protocols, except for WS-Security, provide coarse-grained, point-to-point protection, which is inadequate in the presence of intermediate services. WS-Security, though designed with web service compositions in mind does not address end-to-end security issues, especially in the open environment envisioned by SOC.

Even though there are many architecture available in literature, authors felt that there is a need for research enhancement and development of new architecture for web service security.

III. DESIGN OF WEB SERVICE PLATFORMS

W3C's web services architecture specification specifies the basic framework for WSPs. A WSP is used to mediate interactions between the three entities and this requires support for three basic classes of functionality: exchanging messages, describing web services and publishing and discovering web service descriptions. Since this research addresses the security of information exchanges between the service provider and the client, focus need to be made on the first class of functionality: support for message exchanges.
The Apache Axis2 WSP is one implementation of the web services framework. Axis2 WSP will be used for analysis as not only is it widely used, it is also available under an open source license, enabling us to gain a clearer understanding of its workings [9]. Axis2 provides support for developing, deploying, managing and invoking web services. Additionally, Axis2 also provides support for utilizing many WS-*extensions such as WS-Security and WS-ReliableMessaging.

IV. ARCHITECTURE OF ISO-WSP

The combination of the T-WSP and the U-WSP are called as ISO-WSP. There is separation between the T-WSP and the U-WSP by executing them in separate protection domains, with the U-WSP running with lower privileges. This prevents U-WSP from modifying the binaries or configuration files of the T-WSP. This separation also prevents U-WSP from accessing the secret keys used for encryption or decryption.

A legacy WSP can be converted to an ISO-WSP with a small number of modifications. After constructing a T-WSP, it is need to modify the legacy WSP to invoke the T-WSP via remote invocation mechanisms instead of using local calls. This involves identifying parameters that are exchanged between the T-WSP and U-WSP, message and results of security processing, and adding the necessary serializing and deserializing code. An ISO-WSP prototype can be implemented based on the Apache Axis2 platform

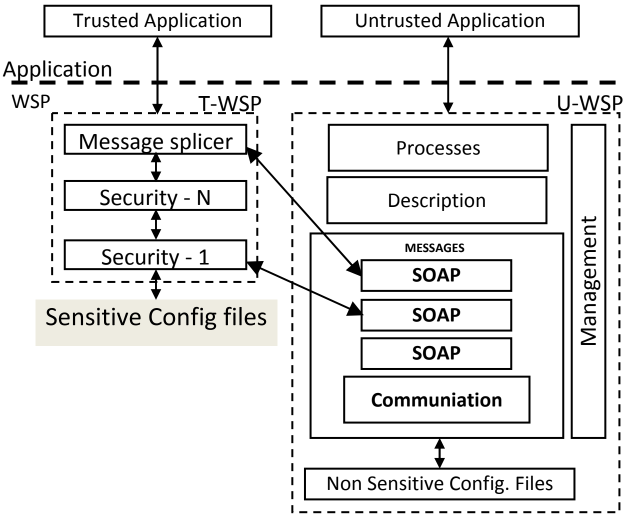

Figure 1 Architecture of ISO-WSP

V. PROPOSED NEW ARCHITECTURE

The design and implementation of WSPs requires users and service providers to trust large and complex components. The configurability and extensibility of many WSPs poses additional challenges to testing and analysis. This has resulted in WSPs with multiple security vulnerabilities.

The ISO-WSP architecture has been developed based on AppCore approach. The AppCore approach has been applied in the WSP architecture to split existing WSPs into two parts: a small, trusted T-WSP that handles security-sensitive information and a legacy, untrusted U-WSP that handles non-sensitive and protected (encrypted or signed) sensitive information.

One potential weakness in the ISO-WSP architecture is that the trusted part now performs operations using data provided by the untrusted part. This may violate the integrity flow in the system, as data is flowing from a lower integrity level (untrusted part) to a higher integrity level (trusted part). We assume that the trusted code validates all inputs from the untrusted part before proceeding with the operation, e.g., by comparing against a local copy.

So it felt that there is a need for research enhancement in existing ISO-WSP architecture. The attempt is being made to develop a new architecture that decomposes the WSPs into three parts executing in the separate protection domain.

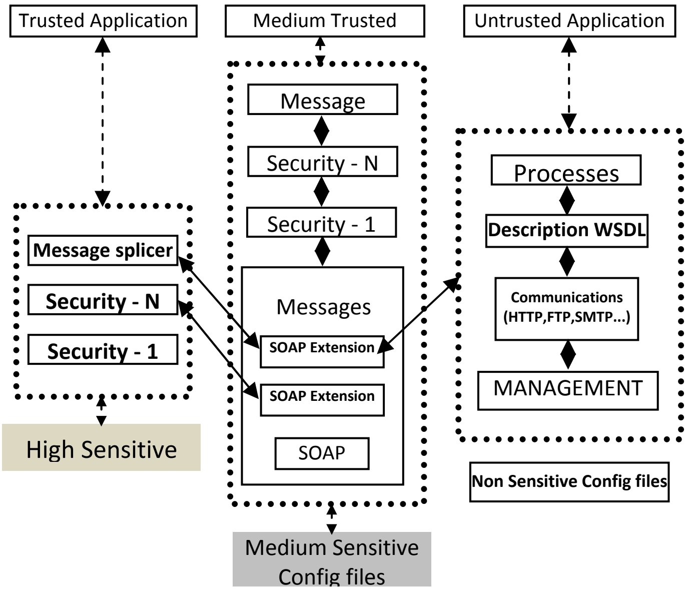

Figure 2 Three-layered WSP architecture

The proposed 3-layered WSP architecture provides the high security than the existing WSP and ISO-WSP architecture.

VI. CONCLUSION

The main objective of this research work has been highlighted. The security problems in existing WSP and ISO-WSP are discussed. The new 3-layer architecture has been proposed to improve the end-to-end security property. The proposed architecture can be modified to provide the automatic separation of data and also this may be implemented with real time web service applications like Health insurance scheme.

REFERENCES

[1] Nils Agne Nordbotten “XML and Web Services Security Standards” IEEE Communications Surveys & Tutorials, Vol. 11, No. 3, Third Quarter 2009 pp:4-21

[2] Jinpeng Wei, , Lenin Singaravelu, and Calton Pu “A Secure Information Flow Architecture for Web Service Platforms” IEEE Transactions on Services Computing, Vol. 1, No. 2, April-June 2008 , pp: 75 - 87

[3] Carsten Rudolph, Nicolai Kuntze, Zaharina Velikova “Secure Web Service Workflow Execution” Elsevier Publications, Electronic Notes in Theoretical Computer Science 33–46 (2009)

[4] Nuno Antunes, Marco Vieira “Comparing the Effectiveness of Penetration Testing and Static Code Analysis on the Detection of SQL Injection Vulnerabilities in Web Services” 15th IEEE Pacific Rim International Symposium on Dependable Computing, 2009

[5] Shenghui Zhao, Guoxin Wu,Yuemin Li , Kun Yu “A Framework for Trustworthy Web Service Management” IEEE Second International Symposium on Electronic Commerce and Security, 2009

[6] Elias Pimenidis and Christos K. Geogiadis “Web services security evaluation considerations” Inderscience Publishers , International Journal of Electronic Security and Digital Forensics, Volume 2 , Issue 3 , 2009, Pages: 239-252

[7] Tomas Knap and Irena Mlynkova “Towards More Secure Web Services” IEEE International Conference on Web Services, 2009

[8] Yin-Soon Loh, Wei-Chuen Yau, Chien-Thang Wong and Wai-Chuen Ho “Design and Implementation of an XML Firewall” IEEE International Conference on Computational Intelligence and Security, Volume 2, 3-6 Nov. 2006, pp:1147 – 1150

[9] S. Perera, C. Herath, J. Ekanayake, E. Chinthaka, A. Ranabahu, D. Jayasinghe, S. Weerawarana, and G. Daniels, “Axis2, Middleware for Next Generation Web Services”, In Proc. ICWS 2006, pp. 833-840, Sept. 2006.

[10] Web Services Trust Language. ftp://www6.software.ibm.com/software/developer/library/ws-trust.pdf Retrieved: 30-Sept-06

[11] Marzouk.S.Mokbel, Le Jiajin ‘Integrated Security Architecture For Web Services And This Challenging’ Journal of Theoretical and Applied Information Technology

[12] Artem Vorobiev and Jun Han Security Attack “Ontology for Web Services” IEEE Proceedings of the Second International Conference on Semantics, Knowledge, and Grid (SKG'06)