DEVELOPMENT OF AN ACCESS CONTROL MODEL FOR WEB SERVICES APPLYING XML-BASED APPROACH

HOMA MOVAHEDNEJAD

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Centre for Advanced Software Engineering (CASE)
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

MARCH 2009

To my beloved husband, sisters, brothers and parents

ACKNOWLEDGEMENT

All praise be to Allah, the Most Merciful, for His Love and Guidance. Salutations on the Prophet Muhammad (PBUH), his family, and fellow companions.

May I express my appreciation to ALLAH, the beneficent, the merciful, for making me a Muslim and blessing me with the privilege of acquiring a higher degree. My heart felt gratitude goes to my parents for bearing with me weakness upon weakness from cradle to date. I am also grateful to my husband because of his uninterrupted support during my study.

I would like to express my sincere appreciation to my supervisor Dr. Maslin Masrom. She has been extremely helpful and offered me all the necessary support needed for success, as such, I owe it a duty to be appreciative. I also appreciate Sayed Hassan Tabatabaei for his continuous support and guide throughout this project. In addition, I wish thank my colleagues Amir, Ala, Hoda, Mojtaba and Atefeh for their support and encouragement. May ALLAH reward you all the relentless efforts to see through this academic pursuit.

ABSTRACT

Web Services is a raising model of Web based applications, which allows interconnection, communication, and interoperability among different devices and applications more convenient. Since web services applications run over the open and unreliable internet, security for web services is a necessity and should be applied to provide services providers and service requestors with quality of protection. With the intention to protect resources and information from unlawful access, access control systems are built to provide protection. In spite of the recent advances in Web based access control approaches applicable to Web Services, there remain issues that obstruct the development of effective access control models for Web Services environment. In this project, a secured model for Web Services to provide an effective Access Control model through strong authentication and authorization has been developed. Moreover, in order to demonstrate the proposed model design, the prototype applying a case study is illustrated.

ABSTRAK

Perkhidmatan web melahirkan model-model applikasi berlandaskan web yang saling hubungan, perhubungan dan saling kendali di antara peralatan dan applikasi yang berbeza dengan lebih mudah. Oleh kerana applikasi perkhidmatan web berfungsi di atas plantar internet yang terbuka dan tidak boleh diharap, keselamatan untuk perkhidmatan web amat diperlukan dan patut diguna-pakai untuk memberikan pembekal perkhidmatan dan peminta perkhidmatan dengan perlindungan yang berkualiti. Dengan tujuan untuk melindungi sumber-sumber dan maklumat daripada capaian yang ditegah, sistem kawalan capaian dibina untuk memberi keupayaan perlindungan. Walaupun terdapat kemajuan baru dalam pendekatan kawalan capaian berlandaskan web, masih terdapat isu-isu yang menghalang pembentukan model-model kawalan capaian untuk persekitaran Perkhidmatan Web. Dalam projek ini, model yang selamat bagi kegunaan Perkhidmatan Web untuk memberikan model kawalan capaian yang berkesan melalui pengesahan dan perakuan kuasa yang kukuh telah dibina. Selanjutnya, untuk mempamerkan cadangan reka bentuk model, satu prototaip menggunakan kes kajian dipaparkan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

API	-	Application Programming Interface
COM	-	Component Object Model
DCOM	-	Distributed Component Object Model
DoS	-	Denial of Service
GUI	-	Graphical User Interface
IDE	-	Integrated Development Environment
IE	-	Internet Explorer
IETF	-	Internet Engineering Task Force
Iniperm	-	Initial Permission
JDK	-	Java Development Kit
J2EE	-	Java Enterprise Edition
JSP	-	Java Server Pages
NC	-	Network Computers
OMG	-	Object Management Group
ORBs	-	Object Request Brokers
ORPC	-	Object Remote Procedure Call
OSI	-	Open Systems Interconnect

PDP	-	Policy Decision Point
PEP	-	Policy Enforcement Point
PGP	-	Pretty Good Privacy
PKI	-	Public Key Infrastructure
QoS	-	Quality of Service
RBAC	-	Role Based Access Control
SAML	-	Security Assertion Markup Language
SJSAS	-	Sun Java System Application Server
SOA	-	Services Oriented Architecture
SOAP	-	Simple Object Access Protocol
SSL	-	Secure Sockets Layer
UDDI	-	Universal Description Discovery and Integration
VPN	-	Virtual Private Network
WS	-	Web Services
WSDL	-	Web Services Description Language
W3C	-	World Wide Web Consortium
XACML	-	Extensible Access Control Markup Language
XKMS	-	XML Key Management Specification
XrML	-	Extensible rights Markup Language

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

Web Services are a transformational technology for integrating information sources from both inside and outside an enterprise [5, 7]. Web Services are the newest incarnation of middleware for distributed computing. Unlike all previous forms of middleware, however, this is a simpler, standards-based, and more loosely coupled technology for connecting data, systems, and organizations. “That is good news for developers and architects wanting to rapidly become expert in this technology and develop real systems. It is also somewhat bad news for them because all middleware needs strong security practices, and Web Services need it more than any middleware of the past” [11]. In addition Web Services create loosely coupled integrations. Web Services are not just being used to integrate internal systems, but they are also integrating data sources from outside the organization [20]. Also Web Services are based on the passing of readable and self-describing business messages represented in XML. Moreover Web Services are based on basic web technologies that already had their own set of security challenges.

1.1. Background of the problem

As mentioned above, owing to wonderful growth of internet-based distributed application and the related increase of computer crime, security is recognized as one of the most serious to individuals, companies and countries. Web Services application run over the open, untrustworthy internet and Web Services providers and requestors must assure their established communication path is not cooperated. In other words, they must ensure the confidentiality and authentication and

authorization of message in transit [9, 2, 19]. Also, as mentioned in IBM and Microsoft joint security white paper [9] security has been a key factor that was holding companies back from adopting Web Services. There are several security issues that must be considered such as confidentiality, integrity, privacy, authentication, authorization, and auditing [22]. So, security for Web Services is a necessity and should be deployed.

1.2. Statement of the Problem

Since new threads and vulnerabilities are introduced to Web Services "what kind of security does Web Services need?" It is seen Web Services security focuses on the application layer, although security at the lower layers remains important. Also, it is discussed the principles of security are confidentiality, authentication, authorization, integrity, non repudiation, privacy, and availability. These are the check boxes that need to be kept in mind when designing a secure system. If only some of the boxes are checked, security loopholes exist [20].

Web Services security present many challenges. One of the hot issues in Web Services security which is considered in this research is the design of effective Access Control schemes that can adequately meet the unique security challenges posed by the Web Services paradigm. In fact, the main question that this research is intended to response can be described as follows:

How to enable Access Control for Web Services environment with respect to authentication, authorization to increase the quality of service (QoS)?

In order to be able to answer this question, a set of research questions that address the problem in detail are defined, as follows:

- **RQ1:** How to use SAML in order to protect transport and request XACML schema instances and other information needed by an XACML implementation?
- **RQ2:** How to deal with the relationship between SAML and XKMS in order to Support trustworthiness?

- **RQ3:** How to specify the interaction between SAML, XACML, and XKMS to support authentication and trust in the SOAP (Simple Object Access Protocol) technology?
- **RQ4:** How to combine the role based and complex context-aware authorization policies with SAML and XACML?

1.3. Project Aim

The aim of this project is to develop an effective Access Control model to provide powerful authentication and authorization in Web Services through the current XML-based technologies and mechanisms.

1.4. Objective of the Study

Project objectives can be listed as follows:

- To investigate security problems in Web Services.
- To evaluate of state-of-the-art approaches base on Access Control using Quality of Service (QoS) criteria.
- To develop effective Access Control model based on XML.
- To validate the proposed model applying a prototype.

1.5. Scope of the Study

The project scope is limited to the security solutions using xml as they can be practically implemented later in development phase, therefore the others security solution is ignored. The design is constructed in a way that contains the best related offered solutions and in the same time be more comprehensive than the others. In addition, the input data to validate the prototype to be applicable are based on a

number of Web Services. In fact, the knowledge base (repository) is assumed as closed world (not open world)

1.6. Significance of Study

- Access control is of increasing importance in a world in which computers are ever-more interconnected through networks. In order to protect resources and information from illegal access, access control systems are built to provide the ability of protection. Access control systems usually implement access control policies [23].

- One of the most important features of Web Service is ease of access over the Internet. But the downside is that security is compromised [1].

- Authorization systems today are increasingly complex. They span domains of administration, rely on many different authentication sources, and manage permissions that can be as complex as the system itself. worse yet, while there are many standards that define authentication mechanisms, the standards that address authorization are less well defined and tend to work only within homogeneous systems [13].

1.7. Summary

With the fast growth of internet-based distributed applications and the associated increase of computer crime opportunities, security is now recognized as one of the most fundamental issues for the computer industry. Web Services is an emerging model of Web-based applications, which makes the interconnection, communication, and interoperability among different devices and applications more convenient. Because Web Services applications run over the open, untrustworthy internet, security for Web Services is a necessity and should be deployed to provide services providers and service requestors with quality of protection.

In this project, a secured model to provide an effective Access Control model through strong authentication and authorization applying for Web Services is developed. There are number of solutions to answer discussed problems such as WS-Security, XML encryption, XML signature, SAML, XACML, XKMS and the like.

REFERENCES

[1] Liu, P. and Chen, Z. An Access Control Model for Web Services in Business Process. *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence 2004(WI 2004)*, September 20-24, 2004. *IEEE /ACM.2004.* 292 – 298.

[2] I,Singh, S. Brydon, G. Murray, V. Ramachandran,T. Violleau. and B.Stearns. *Designing Web Services withJ2EE 1.4 Platform*. 2004.ACM.2004.154-162

[3] Bloomberg.and J. Schmelzer. *A Guide to Securing XML and Web Services*, .2004. Available on : http://ww.zapthink.com

[4] A.Nadalin, C. Kaler, P. Hallam-Baker.and R. Monzillo.OASIS *Web Services Security: SOAP Message Security1.0 (WS-Security 2004)*, Mar. 2004. OASIS Standard200401. Available on: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf.

[5] PerfectXML L.com. *Web Services Introduction*.2004. Available on: PerfectXML .com, http:llwww.~erfectxml.comNVebSv1c. asp.

[6] Erik. C, Francisco. C, Greg Meredith.and Sanjiva W. *Web Services Description Language (WSDL)* .W3C Note 15 March 20001.http://www.w3 .ordTR/wsdl.

[7] *Securing Web Services-Concepts, Standards> and Requiremelzts*. Sun .Microsystem.2003.

[8] *WSDL and UDDI*. Refsnes Data 2005. Available on: http://www.w3schools.com/wsdl/wsd1 uddi.asp.

[9] *Security in a Web Services World: A Proposed Architecture and Roadmap*. IBM and Microsoft April, 2002. Available on: http://www-l06.ibm.com/developer works/web services/libra~y/wssecmapl.

[10] Wolter Roger. *XML Web Services Basics*. Microsoft Corporation. 2001. Available on: http:// msdn. microsoft.co m //Libran //defa t ~ -us/dnweb srv/html/webservbasics.asp.

[11] *Web Sevices SecuritySpeczjkation*. Microsoft, IBM. and VeriSign .2002. Available on: http://www- 106.ibm.com/develo~envorks/webservices/ls -secure/.

[12] Bloomberg J. and Schmelzer R.. *A Guide to Securing XML and Web Services* .ZapThink White Paper, 2004. Available on: www.zapthink.com

[13] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D.R. Kuhn. and R.Chandramoult. Proposed NIST Standard for Role-Based Access Control.*ACM Transactions on Information and System Security*. August 2001. Vol. 4,No. 3: pp. 224-274.

[14] *Extensible Markup Language (XML) 1.0 (Third Edition)*. W3C Recommendation 04 February 2004. Available on: http:I/www.w3 .ordTR/REC-xmV#sec-intro.

[15] B. Galbraith, W.Hankison, A.Hiotis, M.Janakiraman,Prasad D. V., R. Trivedi, D. Whitney. and V. Motukuru. *Professional. Web Services Security*. Wrox Press Ltd., 2002.

[16] *IBM Websphere Studio Application Developer Integration Edition Version 5.0 Getting Started*. IBM Gorp.2003

[17] King. S. Threats and Solutions to Web Services Security. *Network Security*. 2003. 232(6).

[18] J, Rosenberg. and D. L, Remy. *Securing Web Services with WS-Security*. Sams Publishing. 2004.

[19] Microsoft Corporation. *Web Services Enhancements (WSE) 2.0*. 2004. Available on: http://msdn.microsoft.com/webservices/building/wse/default.aspx.

[20] Mark, O'Neill. *Web Services Security*. McGraw-HillIOsborne. 2003

[21] Sang Sing. *Secure Web Services*. Available on: http://www. iavaworld.com/iavaworld~iw-03-2003/iw- wssecurity.htm1

[22] *Web Services Security: SOAP Message Security 1.0*. WS-Security 2004. OASIS Standard 200401.March 2004. Available on: http://docs.oasis-open.ordwss/2004/1l 0o asis-20040 1- wss-soapmessage-security-] .O.pdf.

[23] W. D. Yu. *An Intelligent Access Control for Web Services Based on Service Oriented Architecture Platform*. Software Technologies for Future Embedded and Ubiquitous Systems, 2006 and the 2006 Second International Workshop on Collaborative Computing, Integration, and Assurance. SEUS 2006/WCCIA 2006. The Fourth IEEE Workshop on.27-28 April 2006 Page(s):6 pp.

[24] Rosenberg, J. and Remy, D. *SecuringWeb Services with WS-Security - Demystifying WS-Security. WSPolicy,SAML, XML Signature, and XML Encryption.* Indianapolis, Sams Publishing.2004.ISBN: 0-672-32651-5.

[25] Jothy R. and David R. *Securing Web Services with WSSecurity: Demystifying WS-Security, WS-Policy,SAML, XML Signature, and XML Encryption*. Sams.2004.

[26] McDaniel, G. *Understanding Web Services: XML, WSDL, SOAP and UDDI*. IBM Dictionary of Computing. New York, NY: McGraw-Hill, Inc., 1994. ISBN: 0070314896Newcomer, E. 2002. UK: Addison-Wesley. ISBN:0-201-75081-3.

[27] Anura, G. *Web Services: Theory and Practice*. Digital Press.2004

[28] S.Cantor, J.Kemp. and E. Maler. *Assertions and Protocols for theOASIS Security Assertion Markup Language (SAML)* V2.0. Available on: "http://xml.coverpa~es.or~ni2004-190-8a-.1 1tml

[29] A. Anderson. and H. Lockhart. SAML 2.0 profile ofXACML. *OASIS TC Working Draft*. 2004. Dec 6.

[30] *WS-Security Web Service Security-UsernameToken Profile 1.0. Available in the Internet (050406)*. 2004. Available on: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0.pdf

[31] *eXtensible Access Control Markup Language (XACML)*. Feb 2005.Available on: http://docs.oasis-open.org/xacml/2.0/

[32] *WS-Security Web Service Security-SOAP Message Security1. (WS- Security)*. 2004. Available on: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

[33] E. Damiani, S.D.C di Vimercati, S. Paraboschi. and P.Samarati, Fine grained Access Control for SOAP e-services, *In Proceedings of 10th International Conference on World WideWeb (WWW)*, Hong Kong:W3C.2001. pp. 504–513.

[34] S. Hada.and M. Kudo. *XML Access Control Language:Provisional Authorization for XML Documents*.October16, 2000.Tokyo Research Laboratory, IBM Research.

[35] *A Brief Introduction to XACML*. Available on: http://ww.oasis- open. ordcom1nittees/download.p1p*I3/12*

[36] R,Wonohoesodo. and Z, Tari. A Role based Access Control forWeb Services. *2004. (SCC 2004). Proceedings. 2004 IEEE International Conference* . 15-18 Sept, 2004. Page(s):49 - 56

[37] S,Hai-bo. and H, Fan. An Attribute-Based Access Control Model for Web Services. *Parallel and Distributed Computing, Applications and Technologies*.2006. PDCAT '06. Seventh International Conference .Dec,2006 .Page(s):74 - 79

[38] C.D,Wang. T, Li. and L.C, Feng. Context-aware Environment-Role-Based Access Control Model for Web Services.*e-Business Engineering* 2005. ICEBE 2005. IEEE International Conference .18-21 Oct. 2008 Page(s):220 - 223

[39] V. S, Mewar, S, Aich ,and S, Sural. Access Control Model for Web Services with Attribute Disclosure Restriction, Availability, Reliability and Security. 2007. ARES 2007. The Second International Conference .10-13 April 2007 Page(s):524 - 531

[40] Jimei .Wang.and Lianfu .Jin. Research and Resolution on Web Service Security. *Computer Applications and Software*. February, 2004. No12, Vol 21: 91-93.

[41] H. Yin.J. Zhou, H. Wu, and L. Yu.A SAML/XACML based Access Control between Portal and Web Services. *Data, Privacy, and E-Commerce,* ISDPE 2007. The First International Symposium .1-3 Nov. 2007 Page(s):356 - 360

[42] H. Yin, D. F. McMullen, M. Pierce, K. Huffman, G. Fox and S. B. Barahona, *A PERMIS-based Authorization Solution between Portlets and Back-end Web Services*. In Proceedings of 2nd International Workshop on Grid Computing Environment (GCE06). Florida. U.S.A.,November 2006.

[43] Requirements and Specifications Carnegie Mellon University 18-849b Dependable Embedded Systems Spring 1999 Author: Eushiuan Tran.

[44] Dena Taylor, Director, Health Sciences Writing Centre. and Margaret Procter, U of T Coordinator of Writing Support for use at the University of Toronto. Available on: http://www.utoronto.ca/writing

[45] *XML Key Management Specification 2.0(XKMS)*. 10 March 2002. Available on: http://www.w3.org/TR/xkms2/

[46] M . ARahaman, R. Marten, A. Schaad. *An Inline Approach for Secure SOAP Requests Early Validation and*, Available on: http://www.owasp.org/images/4/4b/AnInlineSOAPValidationApproach-MohammadAshiqurRahaman.pdf

[47] D Box. *Simple Object Access Protocol (SOAP) 1.1*.World Wide Web Consortium (W3C), May 2000. Available on :http://www.w3.org/TR/SOAP

[48] SOAP v1. 2007. Available on: http://www.w3.org/TR/soap12-part1

[49] Rajesh, S. and D. Arulazi. *Quality of service for Web Services– demystification, limitations, and best practices*.

[50] Kreger, H. *Web Services Conceptual Architecture (WSCA 1.0)*. IBM Software Group. Available on the Internet (040121). 2001. Available on: www.306.ibm.comlsoftware/solutions/webservices/pdf/WSCA.pdf

[51] Lili .Sun.and Yan Li. *XML and Web Services Security.IEE.* 2008 .

[52] David F.Ferraiolo. and D.Richard Kuhn(2006). *Role-Based access control*. (2th ed). Library of Congress Cataloging-in-Publication Data: ARTECH HOUSE, INC.

[53] Rafae ,B.Elisa,B.and Arif, G(2004).A Trust-based Contex-Aware Access Control Model for Web Services.*Proceeding of the IEEE International Conference on Web Services(ICWS'04).* 6-9 July . 184 - 191.

[54] Shen,H. and Hong.f(2005).A Context-Aware Role-Based Access Control for Web Services. *Proceeding of the IEEE International Conference on e-Business Engineering(ICEBE'05).* 12-18 Oct. 220 – 223.

[55] Ferraiolo, D.F. and Kuhn, D.R. (October 1992). Role Based Access Control.*15th National Computer Security Conference*. 554-563

[56] Norman H. Cohen, James Black, Paul Castro, Maria Ebling, Barry Leiba,Archan Misra, Wolfgang Segmuller. *Building Context-Aware Applications with Context Weaver.* IBM Software Group.October 22.Available on: http://domino.watson.ibm.com/library/CyberDig.nsf/home.

[57] Joons.Park(2006).*Secure Attribute On The Web*.Ph.d.Thesis.Georg Mason Univercity.

[58] Chaowang,S.Zongkai,Y.Qingtang,L.and Chengling.z(2008). A cotaxt Based Dynamic Access Control Model for Web Service. *IEEE International Conference on Embedded and Ubiquitous Computing.* 17-20 Dec. 339 - 343

[59] Erber, R. Schlager, C.Pernul, G(2007). Patterns for Authentication and Authorisation Infrastructures. *18th International Workshop on Database and Expert Systems Applications.* 3-7 Sept. 2007 .755 – 759.

[60] Junzhe Hu .and Alfred C. Weaver. Dynamic, Context-Aware Access Control for Distributed Healthcare Applications. Available on : www.cs.virginia.edu/papers/p1-hu-dynamic.pdf

[61] Assadarat, Khurat. And Joerg, A(2008). A Mechanism for Requesting Hierarchical Documents in XACML. *IEEE International Conference on Wireless & Mobile Computing, Networking & Communication.* 12-14 Oct. 202 – 207

[62] *Sun Java System Application Server Platform Edition 9 Installation Guide*,Nov 2006. Available on: http://www.sun.com/software/products

[63] Adam, Myatt. *Pro NetBeans™ IDE 6 Rich Client Platform Edition.* Apress. 2008