Chapter 8.12
Using Web Service Enhancements to Establish Trust Relationships with Privacy Protection:
(Extended and Invited from ICWS 2006 with id 47)

Zhengping Wu
University of Bridgeport, USA

Alfred C. Weaver
University of Virginia, USA

ABSTRACT

The lack of effective trust establishment mechanisms impedes the deployment of diverse trust models for web services. One issue is that collaborating organizations need mechanisms to bridge extant relationships among cooperating parties. We describe an indirect trust establishment mechanism to bridge and build new trust relationships from extant trust relationships with privacy protection. Another issue is that a trust establishment mechanism for web services must ensure privacy and owner control. Current web service technologies encourage a service requester to reveal all its private attributes in a pre-packaged credential to the service provider to fulfill the requirements for direct trust establishment. This may lead to privacy leakage. We propose a mechanism whereby the service requester discovers the service provider's requirements from a policy document, then formulates a trust primitive by selectively disclosing attributes in a pre-packaged credential to negotiate a trust relationship. Thus the service requester's privacy is preserved.

INTRODUCTION

Web services facilitate collaborations and inter-operations between business partners, software

agents, service providers and consumers, which promote loosely coupled and dynamic service-oriented architectures. But they do not address the business aspects of interactions such as security, access control, business partner selection, service level agreement monitoring, and auditing – the activities that build trust between a consumer and a provider of a web service and that will ultimately determine which services are used and which are not. The issues of trustworthiness are tightly bound in the minds of consumers. For example, a consumer would generally trust the Citibank online services to conduct online banking in a secure and responsible manner, because Citibank has a massive physical network of banks and has been in the financial market over one hundred years. On the other hand, a consumer probably wouldn't entrust his/her savings to a newly launched financial institution with no obvious connections to any legitimate business. The point here is that as web services begin to gain a foothold in electronic business, critical services will probably be limited to extensions of pre-existing business relationships with already trusted companies.

How can a business service provider engender new trust or transfer trust to a new consumer via an existing agent? And how can two companies establish a trust relationship in order to provide and consume business services or share information over web services? They have to negotiate in order to establish a conventional business trust relationship, and so they would almost certainly want to do the same for a trust relationship using web services. Web service standards UDDI (Atkinson, 2003), WSDL (Christensen, 2001), and SOAP (Box, 2000) say nothing about this. Thus, although it would be possible to find a web service to use just by examining a UDDI registry, it is unlikely to be used prior to investigation of its reputation and reliability. To establish a trust relationship, the consumer and the service provider require a negotiation process. The negotiation process needs to exchange trust-related information between the two parties. The parties can

exchange private attributes to build the trust relationship directly, or they can use pre-established relationships to build a new one via a trusted third party. Exchange of private attributes may put the privacy of the consumer and the service provider at risk. For example, a hacker may pretend to be a consumer to access useful information from the service provider. More seriously, a hacker can pretend to be a service provider to gather private attributes from consumers for malicious usage. We need to reduce that risk. As an alternative, using pre-established relationships may be a more convenient and more secure way.

To provide additional functionalities for security, privacy and many other purposes, "web service enhancements" appear. Web service enhancements are a series of specifications describing security, privacy and other contexts applied to web services by several industrial practitioners. In this article we describe an indirect trust establishment mechanism using web service enhancements for bridging extant trust relationships to produce new trust relationships. Using an exchange of privileges obtained from a commonly trusted third party (who has established trust relationships with both parties) avoids disclosure of any private attributes. Meanwhile this mechanism still allows free negotiation and trust agreement selection between the involved parties when subjective judgments have to be made. We also propose a privacy protection mechanism that reveals the minimal number of attributes necessary to build the desired trust relationship for the web service environment. Using this mechanism, a set of attributes signed by the service requester's digital signature is associated with a trust primitive element. This element is used to negotiate a trust relationship. Any changes of policy requirements associated with this trust relationship are dynamically enforced using a trust group element. The Related Work section provides an overview of related work. The next section, Using Web Service Enhancements To Bridge Trust Relationships, describes how to use web service enhancements

Related Content

FLCEER: Fuzzy Logic Cluster-Based Energy Efficient Routing Protocol for Underwater Acoustic Sensor Network
Sathishkumar Natesanand Rajakumar Krishnan (2020). *International Journal of Information Technology and Web Engineering (pp. 76-101).*
www.irma-international.org/article/flceer/258740

Programmable Implementation and Blockchain Security Scheme Based on Edge Computing Firework Model
Bao Yi Qin, Zheng Haoand Zhao Qiang (2021). *International Journal of Information Technology and Web Engineering (pp. 1-22).*
www.irma-international.org/article/programmable-implementation-and-blockchain-security-scheme-based-on-edge-computing-firework-model/272025

Microclustering-Based Multi-Class Classification on Imbalanced Multi-Relational Datasets
Hemlata Pantand Reena Srivastava (2022). *International Journal of Information Technology and Web Engineering (pp. 1-13).*
www.irma-international.org/article/microclustering-based-multi-class-classification-on-imbalanced-multi-relational-datasets/304053

Saving Face in Online Learning: New Directions in Teaching and E-Learning
Lena Paulo Kushnirand Kenneth Berry (2015). *Artificial Intelligence Technologies and the Evolution of Web 3.0 (pp. 167-187).*
www.irma-international.org/chapter/saving-face-in-online-learning/127288

Research on Fault Diagnosis Method Using Improved Multi-Class Classification Algorithm and Relevance Vector Machine
Kun Wu, Jianshe Kangand Kuo Chi (2015). *International Journal of Information Technology and Web Engineering (pp. 1-16).*
www.irma-international.org/article/research-on-fault-diagnosis-method-using-improved-multi-class-classification-algorithm-and-relevance-vector-machine/145837