Chapter 13
Enhancing Security Modeling for Web Services Using Delegation and Pass-On

Wei She
University of Texas at Dallas, USA

I-Ling Yen
University of Texas at Dallas, USA

Bhavani Thuraisingham
University of Texas at Dallas, USA

ABSTRACT

In recent years, security issues in web service environments have been widely studied and various security standards and models have been proposed. However, most of these standards and models focus on individual web services and do not consider the security issues in composite services. In this article, the authors propose an enhanced security model to control the information flow in service chains. It extends the basic web service security models by introducing the concepts of delegation and pass-on. Based on these concepts, new certificates, certificate chains, delegation and pass-on policies, and how they are used to control the information flow are discussed. The authors also introduce a case study from a healthcare information system to illustrate the protocols.

1 INTRODUCTION

Service oriented architecture (SOA) is a popular paradigm for system integration and interoperation. Web service is the current standard for SOA. While SOA has many benefits, security is still a major concern. Because the web service environment is open, distributed, heterogeneous, and integrated in nature, and involves new processes and messages, new security requirements arise. To fulfill these requirements, a lot of research works have been conducted in recent years to provide better security mechanisms for web service environment. The most notable work is the set of WS security specifications (OASIS, 2006; IBM, 2006) proposed by a group of organizations including

DOI: 10.4018/978-1-4666-1942-5.ch013
OASIS, WS-I, IBM, Microsoft, etc. SAML provides an XML-based standard for the exchange of authentication, entitlement, and attribute information. XACML is the core XML schema defined to represent access control policies. WS Security specifies an abstract web service security model including security tokens with digital signatures to protect and authenticate SOAP messages. WS Trust defines extensions to WS Security, including the methods to issue, renew and validate security tokens, and the way to exchange and broker trust relationships. WS Federation further defines how trust relationships are managed and brokered in a heterogeneous federated environment. WS Trust also supports extended features such as simple delegation and forwarding of security tokens between different parties and exchange of policies. WS Policy specifies a framework for expressing web service constraints and requirements as policies using policy assertions. WS Security Policy extends WS Security by specifying the policy assertions to describe security policies.

The specification models discussed above address the basic security requirements in web services. There have also been other research works that propose innovative security models and extensions to address new security issues in web services. Bhatti et al. proposed to incorporate contextual information, such as time, location, or environmental state, into WS access control models (Bhatti, Bertino, & Ghafoor, 2005). In this model, they also proposed the dynamic trust level of a user, which is initialized by a trust establishing procedure, and adjusted by context in the access. Bertino et al. (2006) proposed to carry on negotiation in an access by specifying the message types and contents exchanged based on the agreement about security requirements and services reached by the requestor and the service provider. In an open environment where unknown users may present, negotiations may also be conducted upon missing credentials or even security policies. Koshutanski et al. (2003) proposed a model that allows the derivation of necessary credentials from a given set of policies. With derived credentials, it is possible to conduct negotiations for privileges. Xu et al. (2006) proposed a framework which allows the negotiation on security policies; that is, even if the user violates part of the policy rules of the service provider, or vice versa, it is still possible to generate a positive access decision if both parties come to an agreement. Skogsrud et al. (2003) proposed to apply the solutions of trust negotiation into web service environments to secure the interactions among unknown users. Rao et al. proposed a security model to secure the process of publishing, searching, and binding a service (2004). In web service environment, security control may also be put on third party brokers (Carminati, Ferrari, & Hung, 2005, 2006), which perform security matchmaking before making further service invocation.

However, most of the existing works focus on individual web services and do not consider service composition. Advanced WS security techniques allow a service to effectively control the accesses to its resources, but do not provide mechanisms to let the services control their further information flows. Consider an online cooperative diagnosis system which involves a patient, several cooperating doctors and counselors, and multiple medical databases. The patient $P$ contacts his family doctor $F$ for help. The symptom of $P$ is unusual and $F$ contacts a specialist $S$ to co-diagnose the disease. After confirmed the diagnosis, $S$ contacts a counselor $C$ to obtain the treatment information and the records of other patients with the same disease, intending to help $P$ understand the treatment information and the records of other patients with the same disease, intending to help $P$ understand the treatment and treatment implications. $C$, in turn, accesses several medical databases $D_i$, $D_2$, $\ldots$, to retrieve the desired information. Assume that $C$ has the full rights to access all the information in the medical databases $D_i$ for some $i$. $C$ trusts $S$ and will pass all obtained results to the specialist $S$. $S$ trusts her college family doctor $F$ and $F$ trusts her patient $P$ and the retrieved medical records will be passed from $S$ to $F$ and to $P$. However, the database $D_i$ may have a policy that the personal