Seamlessly Securing Web Services by a Signing Proxy

Mario Jeckle
University of Applied Sciences, Furtwangen, Germany

Ingo Melzer
DaimlerChrysler Research & Technology, Germany

ABSTRACT

Web services offer a way for very different systems to collaborate independent of the programming language used or the involved operating systems. Their basis is the XML-based SOAP protocol, which can be used over any protocol that is able to transport a byte stream. Due to the fact that Web services do not depend on any operating system and there is no burden of a underlying paradigm, they are ideal for the integration of even completely inhomogeneous systems. However, SOAP does not (and does not have to) deal with security issues, which is nevertheless important for the involved systems. This article describes an add-on for existing Internet proxies to achieve user and developer transparent security features for Web services. This approach allows corporate firewalls to handle authentication. A first step is to add corporate signatures to all outgoing SOAP messages to enable a corporate trust relationship. A second improvement is to use proxy authentication as defined in RFC 2616 and RFC 2617 to add personal signatures assuming that the proxy has access to some key management system.

Keywords: proxy pattern; security; SOAP; Web services.

INTRODUCTION

Today’s computer systems are extremely inhomogeneous, which can be a real burden when collaboration is desired or even required. A possible solution to this problem is Web services, which offer a great possibility for companies and institutions to implement general interfaces to their heterogeneous systems. This allows others, humans or computer systems, to access important information to enable a better cooperation.

However, at the same time, the introduction of Web services for accessing possibly critical business systems may offer other users of the Internet the possibility to gain access to those systems. Most of the time, Web service deployment is based on the well-known HTTP protocol as transport media. Content of this type is normally not inspected or filtered by most firewalls at all. The efficiency of a firewall is therefore significantly reduced. Also, SOAP, the lightweight XML-based protocol of Web services, does not come with
any security features, although a firewall or proxy is a commonly used security facility.

However, this does not constitute SOAP-based Web Services as a general security hole. SOAP is not secure or insecure — security is simply not its job! According to SOAP’s underlying philosophy, the application has to take care of this topic. Taking XML’s co-standards encrypting and digitally signing into account, arbitrary SOAP calls could be secured with respect to privacy, authentication, non-reputation, and integrity of the transmitted data. Based on this, the receiver is able to grant authorization to the system’s access. Since the creation of a secured message requires modifications to the message itself by adding security information, the application creating the SOAP payload is required to be modified as well.

An alternative to changing numerous business systems to introduce security at this protocol layer is presented here. For reasonable secured and closed environments like today’s intranets behind corporate firewalls, it is possible to concentrate the handling of digital signatures at a single point within the network’s structure. The machine devoted to this task could sign and encrypt if desired all outbound Web service calls, and vice versa, decrypt and check the inbound calls as part of corporate’s security infrastructure. Therefore, the inclusion of such a facility will disburden applications and even leverage the usage of security mechanisms. As an option, such a facility could reside on a firewall or proxy machine.

Such an add-on to the proxies can be a service that signs all outgoing SOAP calls with a signature owned by the company or encrypts selective message contents to be readable only for the desired reader. On the other side, the firewall of the other partner will block all SOAP calls that do not have an appropriate signature or cannot be decrypted successfully. The key issue of authorization based on authentication can therefore be eased significantly whenever a call passes an enterprise’s boundary.

This article first illustrates a typical infrastructure for most Web services. It also provides the necessary basics of Web services security and digital XML signatures. Based on this, the most important steps for implementing such a proxy for Web services, which will be termed a **signing proxy**, to achieve a federated or corporate trust are shown.

Secondly, this step will be improved to add personal signatures. For this goal, it is necessary that the proxy is able to identify each user, which can be achieved by using proxy authentication as described in RFC 2616 and RFC2617 (Fielding, 1999; Franks, 1999). If a key management system is installed and the proxy has access to this system, it can add a second signature to the SOAP header that belongs to the calling user.

Additionally, using the XML co-standard XML-Encryption, it is possible to add privacy to the Web services application by encrypting the outgoing messages. However, due to the fact that it is very difficult to do this transparently for all users, encryption plays only a minor role in this article.
Mashup Service Recommendation Based on Usage History and Service Network
[www.igi-global.com/article/mashup-service-recommendation-based-on-usage-history-and-service-network/108883?camid=4v1a](www.igi-global.com/article/mashup-service-recommendation-based-on-usage-history-and-service-network/108883?camid=4v1a)

A Specification Framework for Big Data Initiatives
[www.igi-global.com/chapter/a-specification-framework-for-big-data-initiatives/217854?camid=4v1a](www.igi-global.com/chapter/a-specification-framework-for-big-data-initiatives/217854?camid=4v1a)