Chapter 5.28
Secure Soap-Based Web Services for Distance Education

K. Komathy
Anna University, India

P. Vivekanandan
Anna University, India

V. Ramachandran
Anna University, India

ABSTRACT

The objective of this chapter is to emphasize the need for an effective security model and its implementation for distributed applications. Online web-based education needs to share the resources dynamically, irrespective of the network and platform on which the services are deployed. A communication protocol called Simple Object Access Protocol (SOAP) provides a platform for interoperability, which holds the key for the reuse and integration needed for tomorrow's sophisticated online learning. The requirements of a diverse population of learners can be met with a flexible system such as SOAP that provides education at anytime from anywhere. SOAP protocol does not include the security of the web transactions it carries and so it is the responsibility of any application to take care of the safety of its critical data being transmitted. This chapter attempts to bring out a comprehensive security model based on cryptographic techniques for the distributed web services connected through a SOAP-RPC based communication network to safeguard sensitive information over the wire. The adaptive nature of this proposed security model, not only considers the protection of an entire web transaction, but also customizes the safety of any fragment of the transaction. This analyzes a possible and an alternate security mechanism to vendor-dependant technologies as applicable to the distributed services.

INTRODUCTION

SOAP is a lightweight protocol for information exchange in a decentralized, distributed environment. It meets the needs of web developers who find distributed computing difficult to deploy with DCOM and CORBA because of firewall protection. SOAP combines the power of Remote Procedure call (RPC) and the flexibility of Extensible Markup Language (XML)(Tim, 2000). The protocol performs RPC using HTTP as the underlying communication protocol and XML as the data serialization format. XML being a text-based, meta-language, rather than binary, promotes platform independence. Ideally, any call that ends up invoking a remote procedure through a network endpoint can be encapsulated in a SOAP Envelope. This includes Distributed Computing Environment (DCE) RPC calls, COM/DCOM calls, CORBA calls, Java calls, etc., which further help SOAP to be a suitable protocol for distributed Web services. Moreover, XML facilitates application of the security mechanisms such as encryption and digital signature to selected fragments of the payload rather than restricting to the entire Web document.

Several security models have been proposed in the literature to support the authorization and access control policies for XML data while in storage. A more recent approach is on the role-based policies that regulate the access to the information based on the activities that the users execute in the system. Several flexible models (Ferraiolo, 1999; John, 1996; Sandhu, 1996) have been discussed and brought out based on this approach. The World Wide Web consortium has also released a draft proposal (Marchiori, 2000), which enables Web sites to express their privacy practices in a standard XML format that can be easily retrieved and interpreted by any user agent. Access control mechanisms for the web-based framework to manage the XML information, proposed by Damiani et al. (Damiani, 2001, 2002) restrict the access on the structure and as well as the content of the XML documents. Kudo and Hada (2000) have proposed an access control system for XML documents where optional provisional actions are included in the specification of each authorization. A provisional action is defined on a set of functions such as log, verify, encrypt, transform, write, create, and delete.

Need for SOAP Security

Various proposals from both industry and academia are dedicated towards the authorization and access control policies for safeguarding the XML information system stored at the server. Secure data transmission is not discussed in most of their designs, as their models rely on the existing security technology such as Secure Socket Layer (SSL). SOAP works as a communication protocol between the application layer having HTTP and user application having the business data, providing independence for application and language. SOAP 1.1 specification (Don, 2000), however contains no details about the security issues like integrity and privacy of messages. The SOAP 1.2 specification (Hugo, 2002) submitted to the W3C calls for future work on SOAP security binding framework and the XML Protocol Working Group has just started the formal work on this. Presently, security for SOAP protocol is provided through the contemporary technologies over HTTP such as SSL (Alan, 1996), Transport Layer Security (TLS) (Dierks, 1999), Internet Protocol Security (IPSEC) (Atkinson, 1995) and Firewall. These technologies may provide adequate security in some network settings but do not meet all messaging security requirements in the web services framework. Indeed, both firewall filtering of HTTP headers and the secure cookies approach have been conceived for simple document retrieval on the WWW and cannot be considered satisfactory for remote invocations. Access to Web services requires a more sophisticated security