

A Distributed Security Framework for Accessing Composite Web Services

Hassina Nacer

Department of computer science
University A/Mira of Bejaia, Algeria
Laboratory LIMED
Sino_nacer@yahoo.fr

Abstract

The Web services technology opens a new dimension and becomes a foundation technology for developing and integrating distributed applications in a loosely-coupled, language-neutral and platform-independent way. However, proliferation of Web services based applications, collaboration and interoperability between companies, extremely heterogeneous policies of security, and, more generally, reply attacks over Internet are major challenges in the design of security infrastructures for Web services. In this paper, we focus our study on security of composite Web services. We propose a distributed model of security for composite Web services which has several functionalities. First, it ensures authentication for arbitrary virtual Web services over Internet. Second, it can process across and beyond domain authentication boundaries. Third, it takes over the conflicts of security policies. Furthermore, the model is scalable and dynamic because it is designed in a fully distributed manner, there are no central points and it evolves over time. An implementation of a prototype and a simulation design demonstrate that a strong security can be achieved for both the client and the virtual Web service through the combination of a dynamic and collaborative trust model with a number of enhancements: (i) a combined encryption technique, (ii) a distributed authority of certificates, and (iii) semantic annotations.