Seamlessly Securing Web Services Using Policies

Mifla Mashood, Gihan Wikramanayake
University of Colombo School of Computing
mifla17@gmail.com, gnw@ucsc.cmb.ac.lk

1. Introduction

As Web Services begin to dominate the market of distributed computing, securing the pipelines from intruders is becoming a mission, which cannot be considered as trivial anymore. In today's highly competitive world, businesses adopt web services due to its very attractive features like platform independency, unprecedented support from major vendors, ability of seamlessly interfacing with legacy systems, use of standardized protocols (SOAP, XML, UDDI, WSDL etc…) etc…As a result they unsuspectingly expose themselves into a zone filled with security loop holes which can pose a great threat to confidential data which might be travelling through the channels using these services.

This paper intends to propose a comprehensive security solution for securing web services through the use of policies, which can be easily incorporated into the existing infrastructures with minimum cost and effort on the part of the developers and businesses.

2. Problem definition

In this era of IT where SSL is considered as a pioneer in securing communication lines against encroachments of many kinds, the most obvious question anyone would pose is, why not use SSL to secure web services? Although it might seem as a valid argument at the onset, SSL used alone, does not provide a comprehensive security solution for web services. Thus, various XML-based security initiatives are in the works to address Web services' unique security needs.

3. A solution using policies

SOAP, the lightweight XML-based protocol of web services does not come with any security features. Taking XML's co-standards encrypting and digitally signing into account, arbitrary SOAP calls could be secured with respect to privacy, authentication, non-repudiation, and integrity of the transmitted data. Based on this, the receiver is able to grant authorization to the system's access. Thus any message level security solution for web services would involve the modification and the apposite interpretation of the SOAP messages. In the solution proposed herein the SOAP payload is modified and interpreted by the use of policy files.

In order to successfully integrate with a policy based web service, one must fully understand the service's XML contract (also referred to as policies). A standard policy framework such as WS-Policy, which forms an integral part of the solution proposed herein would make it possible for developers to express the policies of services in a machine-readable way, enforce them and interpret them. For example, a developer could write a policy stating that a given service requires Kerberos tokens, digital signatures and encryption and others could use the policy information to decide whether they can use the service. Plus, the infrastructure could enforce these requirements without requiring the developer to write a single line of code offering developers a more declarative programming model.

WS-Policy provides a flexible and extensible grammar for expressing policies in a machine-readable XML format. The XML representation of a policy is referred to as a policy expression. A policy expression is bound to a policy subject (e.g., a Web service endpoint). WSE 3.0 by Microsoft has been one of the most effective and widely adopted practical implementation of all these specifications

4. Conclusions and Future Work

Although the proposed solution seem to be ideal in seamlessly integrating security into the existing web service infrastructures it could prove to be a burden on part of the applications, which might require slight alterations in order to incorporate these changes. Thus future work can be channelled through lines where even the applications would be able to transit seamlessly to use these policy files.