dDelega: Trust Management for Web Services

Michele Tomaiuolo, Department of Information Engineering, University of Parma, Parma, Italy

ABSTRACT

In the context of Web services, access control presents some interesting challenges, especially when services are exposed to a global audience, with users accessing them from different systems and under different security settings. A decentralized approach to access control, which can be applied to such open environments, is represented by Trust Management. In fact, it is based on the peer-to-peer delegation of access rights among users, also across organizational boundaries, without supposing a-priori the existence of trusted third parties in the system. This article presents dDelega, a Trust Management framework for SOAP-style and REST-style Web services, available as open source software and usable in different application scenarios. The framework allows users to create multiple levels of delegation of access rights for protected resources. It defines various certificates, for binding names, permissions and oblivious attributes to users, adhering to relevant standards, such as WS-Security, SAML and XACML.

Keywords: Access Control, Authorization, Digital Signature, Extensible Markup Language (XML), Public Key Encryption, Security Management, Web Technologies

INTRODUCTION

The availability of services hosted on the Internet and invoked through open standard protocols allows developers to create modular and adaptive applications. Applications conforming to Web services standards can select and compose services at runtime, crossing both organizational and technological boundaries. In this sense, a standard Service-Oriented Architecture brings many benefits and high promises, in particular from the point of view of improved interoperability among diverse systems. Consequently, the number of open platforms hosting and providing Web services is growing, together with the number of initiatives, platforms and languages aimed at simplifying the integration of existing heterogeneous systems.

With regard to Web services security, a number of protocols and formats have been standardized by various organizations such as W3C, WS-I, OASIS, etc. A basic way of achieving security for Web services is relying on a secure transport layer, typically HTTPS and TLS. However, a message-level security is required in the case of architectures in which intermediaries can manipulate messages on their way. This was the rationale for the definition of new specifications, such as WS-Security. By using the XML-signature and XML-encryption...
specifications, WS-Security defines a standard way to secure SOAP messages, independently from the underlying transport protocol. As far as the REST-style is concerned, the security model is not as highly-developed as the security model for SOAP.

Despite all the efforts, realizing access control for protecting resources and services in an open context is still a challenging task, for both systems developers and system administrators. Moreover, in a global environment, it is not realistic to assume that all authorized principals are known in advance and listed in an ACL or some kind of prefigured policy. Since the recent widespread adoption of the Internet in consumer markets, contacts among people are often fully digitalized and there is still no definite solution to the problem of identity management. Actually, there could be no body of knowledge to associate with a name and the simple idea of building an on-line, global database of names and personal profiles is obviously infeasible as a general solution.

Given such a new way people are using the Internet today, a scheme of authorization based on peer-to-peer trust relationships becomes relevant, because it provides a scalable and easily extensible model to protect a generic resource across organizational boundaries. A possible approach to access control in an open environment is based on decentralized Trust Management (TM), i.e., on the peer-to-peer delegation of access rights among users. In Trust Management systems, in fact, the administrator of local resources is considered as the ultimate source of trust about them, and is provided with means to carefully regulate the flow of delegated permissions. No a-priori trusted parties are supposed to exist in the system, in general. This can also represent the basic setting for improved interoperability among diverse systems, paving the way for the realization of federated security infrastructures.

Thus, Trust Management fits well the context of an open Service-Oriented Architecture, for example in the case of composed services or in the presence of intermediaries between the requesters and the resources. In fact, such problems become more complex when the use of workflows involves many layers of services, with the possible presence of intermediaries. In this scenario, at each level an agent is responsible for managing its workflow. It can possibly subdivide its complex task into sub-tasks and set up a negotiation process with some agents responsible for the execution of simpler Web services. From the perspective of this example, two main abstract roles can be distinguished: the Service Manager and the Workflow Manager. In a typical peer-to-peer architecture, each agent can play different roles at different times. Each Service Manager is associated to one or more Web services and is responsible for the interaction with them. The Workflow Manager has the goal of supporting its user in the process of building a workflow. It composes external Web services and monitors their execution. In this sense, the Workflow Manager assumes the role of the delegate agent in a delegation protocol. However, these delegations cannot come into effect unless they are associated with a corresponding delegation of privileges, for accessing needed resources and completing assigned tasks.

This article describes the topic of Trust Management in the context of Web services and presents dDelega, a security framework for both SOAP-style and REST-style Web services that allows the distributed delegation of access rights among different services and clients. The article is organized as follows. The next section provides a literature review about the principles of Trust Management and Automated Trust Negotiation, the use of oblivious attributes for preserving privacy in Trust Negotiation protocols, some relevant examples of access control frameworks proposed for Web services. Then, the dDelega framework is introduced, together with some basic services exploiting its delegation mechanisms. Finally, a balance about this ongoing work is drawn.

**Trust Management**

Apart from the use of Certification Authorities as trusted third parties, which is a quite traditional
Network Intrusion Detection Using Multi-Objective Ensemble Classifiers
[www.igi-global.com/chapter/network-intrusion-detection-using-multi-objective-ensemble-classifiers/152965?camid=4v1a](http://www.igi-global.com/chapter/network-intrusion-detection-using-multi-objective-ensemble-classifiers/152965?camid=4v1a)

Autonomy, Abortion and Pain Criteria: An Ethical Approach
[www.igi-global.com/chapter/autonomy-abortion-pain-criteria/50412?camid=4v1a](http://www.igi-global.com/chapter/autonomy-abortion-pain-criteria/50412?camid=4v1a)