A Classification of Delegation Schemes for Attribute Authority

Ludwig Seitz, Erik Rissanen, and Babak Sadighi
SPOT, SICS
Box 1263, SE-16429 KISTA, Sweden
{ludwig, mirty, babak}@sics.se

Abstract. Recently assertions have been explored as a generalisation of certificates within access control. Assertions\(^1\) are used to link arbitrary attributes (e.g. roles, security clearances) to arbitrary entities (e.g. users, resources). These attributes can then be used as identifiers in access control policies to refer to groups of users or resources.

In many applications attribute management does not happen within the access control system. External entities manage attribute assignments and issue assertions that are then used in the access control system. Some approaches also allow for the delegation of attribute authority, in order to spread the administrative workload. In such systems the consumers of attribute assertions issued by a delegated authority need a delegation verification scheme.

In this article we propose a classification for schemes that allow to verify delegated authority, with a focus on attribute assertion. Using our classification, one can deduce some advantages and drawbacks of different approaches to delegated attribute assertion.

1 Introduction

Attributes are currently regarded as the most generic way of referring to users and resources in access control systems. User identity, group memberships, security clearances, and roles can all be expressed using attributes. The eXtensible Access Control Markup Language (XACML)\(^2\) uses attributes in order to specify applicable subjects, resources and actions in access control policies.

Access control systems are important components of distributed computing infrastructures (e.g. in Grid computing \[2\]). Often such infrastructures allow to share resources belonging to different entities, based on a mutually agreed access control policy. In order to enforce these policies locally for external users, the access control system needs to be capable to fetch attributes from external sources.

In complex cooperative scenarios, where different resources are administrated by different authorities and used by a variety of users, one can increase the efficiency of administration by delegating attribute authority. Delegation helps

\(^1\) We use assertions synonymous for attribute certificates.

© Springer-Verlag Berlin Heidelberg 2007
to spread the responsibility for specific security decisions to the people who are capable and in charge of taking them, instead of burdening a single administrator with it. This makes the system less error prone and makes it faster to implement attribute assignments on a local level.

In such a scenario, the problem arises how to verify whether an attribute assertion is valid and properly authorised. Various approaches for doing this exist, which all have different drawbacks and advantages.

In this article we present a method to classify different verification approaches based on two simple properties and present advantages and drawbacks of the various models based on our classification.

The remainder of this article is organised as follows: In section 2 we give a short overview of background knowledge necessary to reason about authority delegation. Section 3 presents related work. In section 4 we present our classification approach. We then discuss the advantages and drawbacks of the different models that can be obtained from the classification in section 5. Finally we summarise and give a conclusion in section 6.

2 Background

We assume an access control model, where every attribute has a source of authority (SOA), which is the initial entity that has the power to assign this attribute to other users. In our model a SOA can delegate administrative rights concerning the attribute, thus allowing other entities to act as Attribute Authorities (AA). Such a delegation allows an AA to assign attributes to entities and can also authorise further delegation of their authority. The delegation can be subject to conditions specified by its issuer, that constrain the authority it conveys.

The underlying delegation model that we implicitly use is more formally specified in the publications “Constrained Delegation” [3] and “Using Authority Certificates to Create Management Structures” [4].

3 Related Work

Attribute assertion has received intensive attention from the research community in the last years. As a result of this, two competing standards have emerged for issuing attribute assertions. Furthermore several systems using either one of these standards provide attribute assertion services. In this section we first discuss attribute assertion standards and then present some systems that use these standards to provide attribute assertion services.

3.1 Attribute Assertion Standards

The SAML [5] standard by the OASIS consortium defines an XML based syntax and protocols for requesting and providing different kinds of assertions, including attribute assertions. The current core specification of SAML does not address