An Access Control Language Based on Term Rewriting and Description Logic

Michele Baggi, Demis Ballis, and Moreno Falaschi

1 Dip. di Scienze Matematiche e Informatiche
Pian dei Mantellini 44, 53100 Siena, Italy
{baggi,moreno.falaschi}@unisi.it
2 Dip. Matematica e Informatica
Via delle Scienze 206, 33100 Udine, Italy
demis@dimi.uniud.it

Abstract. This paper presents a rule-based, domain specific language for modeling access control policies which is particularly suitable for managing security in the semantic web, since (i) it allows one to evaluate authorization requests according to semantic information retrieved from remote knowledge bases; (ii) it supports semantic-based policy composition, delegation and closure via flexible operators which can be defined by security administrators in a pure declarative way with little effort. The operational engine of the language smoothly integrates description logic into standard term rewriting giving support to reasoning capabilities which are particularly useful in this context, since they allow one to naturally combine and reuse data extracted from multiple knowledge bases. Such a rewrite engine can be used to evaluate authorization requests w.r.t. a policy specification as well as to formally check properties regarding the security domain to be protected. The language we propose has been implemented in a prototypical system, which is written in Haskell. Some case studies have been analyzed to highlight the potentiality of our approach.

1 Introduction

The widespread use of web-based applications provides an easy way to share and exchange data as well as resources over the Internet. In this context, controlling the user’s ability to exercise access privileges on distributed information is a crucial issue, which requires adequate security and privacy support. In recent years, there has been a considerable attention to distributed access control, which has rapidly led to the development of several domain specific languages for the specification of access control policies in such heterogeneous environments: among those, it is worth mentioning the standard XML frameworks XACML [21] and WS-Policy [25]. Nevertheless, the proposed approaches offer a limited support to the emerging semantic web technologies which are very often embedded into

* This work has been partially supported by the Italian MUR under grant RBIN04M888, FIRB project, Internationalization 2004.
modern web applications. More generally, we can affirm that the security impact of such semantic-aware applications have been not sufficiently investigated to date.

In the semantic web, resources are annotated with machine-understandable metadata which can be exploited by intelligent agents to infer semantic information regarding the resources under examination. Therefore, in this context, application’s security aspects should depend on the semantic nature of the entities in play (e.g. resources, subjects). In particular, it would be desirable to be able to specify access control requirements about resources and subjects in terms of the rich metadata describing them.

In this paper, we present a rule-based, domain specific language well-suited to manage security of semantic web applications. As a matter of fact, it allows security administrators to tightly couple access control rules with knowledge bases (modeled using Description Logic (DL) [1]) that provide semantic-aware descriptions of subjects and resources.

The operational mechanism of our language is based on a rewriting-like mechanism integrating DL into term rewriting [2]. Specifically, the standard rewrite relation is equipped with reasoning capabilities which allow us to extract semantic information from (possibly remote) knowledge bases in order to evaluate authorization requests. In this setting, access control policies are modeled as sets of rewrite rules, called policy rules, which may contain queries expressed in an appropriate DL language. Hence, evaluating an authorization request — specifying the intention of a subject to gain access to a given resource — boils down to rewriting the initial request using the policy rules until a decision is reached (e.g. permit, deny, notApplicable).

Since policy composition is an essential aspect of access control in collaborative and distribute environments ([6,13,19,7]), our language is also endowed with policy assembly facilities which allow us to glue together several simpler access control policies into a more complex one. To this respect, our language is expressive enough to model all the XACML [21] composition algorithms as well as other conflict-resolution, closure and delegation criteria.

Finally, it is worth noting that our formal framework is particularly suitable for the analysis of policy’s domain properties such as cardinality constraints and separation of duty. As our rewriting mechanism combines term rewriting with description logic, the analysis of policy specifications can fruitfully exploit both rewriting techniques and DL reasoning capabilities.

**Related Work.** Term rewriting has been proven successful in formalizing access control of systems. For instance, [4] demonstrates that term rewriting is an adequate formalism to model Access Control Lists as well as Role-based Access Control (RBAC) policies. Moreover, it shows how properties of the rewrite relation can enforce policy correctness properties. Also issues regarding policy composition have been investigated within the term rewriting setting. For example, [6] formalizes a higher-order rewrite theory in which access control policies are combined together by means of higher-order operators; then, modularity properties of the theory are used to derive the correctness of the global policy.