INVITED TALK - TOWARDS SEMANTICS-AWARE ACCESS CONTROL

Ernesto Damiani and Sabrina De Capitani di Vimercati

Abstract Semantic-Web style metadata for advanced context representation and domain knowledge are likely to play a more and more important role within access control models and languages. This paper outlines how context metadata can be referred to in semantics-aware access control policies and discusses the main open issues in designing, producing, and maintaining metadata for security.

1. INTRODUCTION

It is widely recognized that a well-understood model and a highly expressive language for access control are of paramount importance in today's global network environment. A common syntax and semantics for specifying and enforcing access control policies makes it possible to express and exchange the conditions under which distributed resources and services can be used in an open environment. Sharing and composing access control policies enables cooperation and federation of distributed services, as required by emerging Web-based computation paradigms. In this paper, we present our recent research work [2], dealing with three key aspects of knowledge representation involved in this new generation of access control languages:

- *Resource representation.* Writing access control policies where resources to be protected are pointed at via data identifiers and access conditions are evaluated against their attribute values is not sufficient anymore. Rather, it is important to be able to specify access control requirements about resources in terms of available metadata describing them.
- *Context representation.* Distributed environments have increased the amount of context information available at policy evaluation time (e.g., location-based one), and this information is achieving a more and more important role.
- *Subject identity.* Evaluating conditions on the subject requesting access to a resource often means accessing personal information either pre-

sented by the requestor as a part of the authentication process or available elsewhere. Identifying subjects raises a number of privacy issues, since electronic transactions (e.g., purchases) require disclosure of a far greater quantity of information than their physical counterparts. A number of alternatives to *strong identities* are coming of age, all of them involving advanced metadata. Recent research work by our group [3] is based on the idea that *reputations* are a resource that can be computed on the basis of the views of a user community about a *pseudonym;* also, reputations can be stored, maintained, and certified.

For metadata to play the fundamental role outlined above, several research problems need to be solved. To begin with, description metadata must be authenticated and aggregated before their content can be used for policy evaluation, and the need to determine metadata *trustworthiness* becomes important. A number of XML-based standards [18] are available that describe resources (including users) and services as well as circumstances and the environment where the transaction takes place. Promising approaches have started to emerge which rely on Semantic Web technologies [28]. The Semantic Web approach represents shared knowledge via standard *ontologies,* that are then used by intelligent agents to understand the nature of the information they are processing [10]. In interoperable e-business architectures based on the semantic web vision, *ontology-based domain models* are used as controlled vocabularies for resources description, allowing users to obtain the right resources at the right time [6]. While research on developing standards and tools that ultimately will lead to the existence of the semantic web is increasing [28], many issues still need to be solved to enable integrating the result of this research into access control languages. For instance, the high expressive power of semantic web metadata allows for using multiple different syntaxes to carry the same semantics. While no constraints can be posed a priori on the content of resources' descriptors, a standard syntax must be adopted for metadata used to describe subjects and objects within access control policies. Also, a standard syntax should be used for subjects' descriptions. In our view, metadata underlying access control, reputation and trust must come together with those aimed at reputation management as the cornerstone of the new generation secure information infrastructure.

1.1 Digital Identities

In today's networked society, business and personal interactions increasingly involve a huge amount of identity-related information in the form of certifications, credentials, and so on. In access control, identity-related data and metadata about subjects enjoy a special status due to privacy concerns. While digital information collected during electronic transactions is important

for correct evaluation of access control conditions, it is also inherently prone to unauthorized user profiling, privacy leaks, and so on. While stricter regulations and technological countermeasures are important, the issue cannot be solved without devising *credential-less* alternatives for carrying out e-business activities. Although the idea of dispensing entirely with credentials, that is, executing transactions using just the information at hand, may look appealing in principle (e.g., a candidate for a job could prove her competence by answering a list of questions or taking part to a simulation, instead of producing a college degree), it turns out to be impractical in most cases. On the other hand, there is an increasing request of restoring full user control over the degree of anonymity to be preserved during electronic transactions. Disclosure of identity-related information is perceived as a matter of negotiation between the parties involved, perhaps requiring compensation. According to this view, identity is a credential like any other and cannot be demanded, only negotiated [4]. While strong identities directly connected to persons and organizations will undoubtedly remain important, current user requirements demand a wider palette of techniques.

1.2 Metadata for Reputation

While disposable one-time session identifiers guaranteeing complete anonymity have been an important success factor for some widespread peer-to-peer (P2P) systems they cannot be considered a viable alternative to strong identities. Disposable opaque identifiers may cause loosing accountability for physical threats and misbehavior, as well as repudiation of debts and obligations. From this point of view, a more realistic alternative is represented by *digital pseudonyms* or *nyms.* While actual identities cannot be deduced easily from them, digital pseudonyms are persistent and can carry reputations and even credentials. Even without a reputation management system, some pseudonyms have established reputable digital personas on the Net and are considered well worth interacting with. Recent research work by our group [3] is based on the idea that reputations are a resource that can be computed on the basis of the views of a user community about a given pseudonym; also, reputations can be stored, maintained, and certified. When coupled with P2P systems, such reputations can substantially increase the accountability of the P2P network infrastructure without requiring the introduction of a system of strong identities. This way, reputation-aware P2P potentially provides a pseudonym-based service and communication channel that complements client-server Web identity-based applications. For instance, credentials will be always needed to reserve a hotel room or to book a airline ticket; on the other hand, a pseudonym is perfectly suitable when the user is collecting information from tourist sites using a P2P client and prefers not to disclose identity at this preliminary

stage. Even within companies and organization boundaries, having communication channels with different degrees of anonymity may prove worthwhile. Pseudonym-based groupware and anonymous brainstorming and voting can facilitate collection (and increase the value) of knowledge within organizations. These systems could initially start in meetings and then be extended to remote sites, and eventually to nationwide and international forums.

1.3 Integrating Metadata Within Policies

Although some preliminary work has been done toward the definition of a semantics-aware access control process (Section 4), virtually no effort has been made toward integrating contributions into standard access control languages. Emerging attribute-based security languages (e.g., XACML) cannot express access restrictions on resources based on metadata like complex semantics-aware assertions. Rather than redesigning access control languages from scratch to accommodate metadata, we put forward the idea of extending current policy languages to allow for defining access control rules based on generic assertions. Integrating assertion-based metadata allows for specifying access control rules about: *i)* subjects accessing the information and *ii)* resources to be accessed in terms of rich ontology-based metadata associated with them. Assertions included in policy rules are built on a vocabulary including domain- and subject-related concepts, respectively.[1] Access control rules are then enforced on resources annotated with metadata built on the same domain vocabulary. The result is a semantic-aware policy language exploiting the high expressive power of ontology-based models.

2. TOWARDS A SEMANRIC-AWARE ACCESS CONTROL LANGUAGE

We briefly outline how current XML-based standards, namely XACML, SAML (the XML standard for encapsulating security information, including access requests) could be extended to seamlessly incorporate RDF metadata about subjects and objects.

2.1 Including assertion-based metadata in XACML

The design of a policy evaluation and enforcement engine exploiting semantic web metadata needs to be based on a sound model and language for expressing authorizations in term of metadata. To this purpose, we chose to exploit the *extensibility points* already built in the XACML language rather

[1]Subject related concepts may well include reputation metadata, reputation processing introduces an additional layer of complexity in policy evaluation. Therefore, for the sake of simplicity, we shall not elaborate further on reputations in this paper.

than redesigning a policy language from scratch. Our extension points can be summarized as follows.

- Extend the `XACML Context` to include metadata associated with both subjects and resources.

- Extend the `AttributeValue` XACML element (used in XACML to qualify both subjects and objects) capability of specifying auxiliary namespaces.[2] Auxiliary namespaces to be added are at least two: the `rdf:` one, allowing for using RDF assertions as values for the XACML `AttributeValue` element and another one (in our example, `md:` and `ms:`) enabling using properties and class names from a user ontology within those assertions.

- Extend the `MatchID` attribute by introducing a new function, called `metadataQuery`, expressing the processing needed for policy enforcement.

Although our proposed extensions to XACML rely on standard RDF syntax, some precautions should be taken to keep the computational complexity of enforcement under control; in our work, we prescribe that attribute values written in RDF use a *RDF reification technique.*

2.2 Incapsulating semantics-aware credentials in SAML

The SAML-XML Schema specifies that the structure of an authentication assertion involves a `Subject` and at least one `Attribute`, in turn holding at least one `AttributeValue` of any type. The attribute definition is extremely open, leaving it to application-specific XML schemata to specify the actual set of attributes identifying the user. We simply extend the attributes allowed for the `AttributeValue` element to enable content including RDF assertions using suitable ontology concepts as predicate names. In the simplest case, the subject metadata can assert that the user holding the certificates belongs to a certain type (e.g., `(thisRequestUser, type, Trainer)`), or more complex ones such as:

```
(thisRequestUser, type, Person)
(thisRequestUser, buys , "Resource")
(Resource, type, MovieDVD)
(Resource, title, "Using a Spreadsheet")
```

However, once again we use a canonical reified syntax.

[2] Such additional attribute values are optional and do not disrupt parsability of standard XACML policies using our extended schema.

```
<rdf:RDF
  xmlns:rdf="http://www.w3.org/TR/WD-rdf-syntax#"
  xmlns:md="http://ourdomain.it/MD/Schema/md-syntax#"
  xmlns:ms="http://ourdomain.it/MS/Schema/ms-syntax#">
  <rdf:Description
    rdf:about="http://ourdomain.it/MD/PresSMIL/presentation7318.smi">
    <rdf:type rdf:resource="http://ourdomain.it/MD/Schema/md-syntax#PresSMIL" />
    <md:title>Conference presentation 2004-02-13</md:title>
    <md:duration>7256992</md:duration>
    <md:format>application/smil</md:format>
    <md:contains>
      <rdf:Bag>
        <rdf:li rdf:resource="http://ourdomain.it/MD/Text/transcript7318.txt"/>
        <rdf:li rdf:resource="http://ourdomain.it/MD/Image/chart457.png"/>
        <rdf:li rdf:resource="http://ourdomain.it/MD/Video/video010234.avi"/>
      </rdf:Bag>
    </md:contains>
  </rdf:Description>
</rdf:RDF>
```

Figure 1. An example of RDF metadata associated with a SMIL presentation

2.3 Using the extended language

To illustrate our examples of semantics-aware access control policies, we shall consider a *digital library* (DL) containing a wide *e-learning objects* composed of different kinds of multimedia data. Each learning object is complemented with metadata in the form of RDF descriptors that can be written using the ontology vocabulary. However, in some controlled environments it might be possible to adopt the reification-based syntax greatly simplifying the evaluation procedure. In the following, we shall assume that the reified format of RDF statements is used. Note that however conversion tools are available capable to translate a variety of RDF syntax into the reified ones.

To express the statements in our descriptors, we use three vocabularies: (1) the RDFS base namespace [27]; (2) a *resource domain ontology* containing domain-specific terms that are used to describe the resource content (e.g., `Video` and `shows_how`); and (3) a *subject domain ontology* containing terms that are used to make assertions on subjects (e.g., `Trainer`, `Trainee`, `instructs`).

Figure 1 illustrates an example of RDF descriptor where, in addition to the classical `rdf:` namespace, we use namespace `md:` for describing multimedia data. The RDF descriptor, associated with a SMIL (`presentation7318.smi`), states that the presentation contains a video, an image, and a text transcription.[3] Consider now the following protection requirement:

> Trainers of the `Teaching Quality Evaluation` group are allowed to see SMIL presentations containing a video that shows trainers instructing trainees.

This requirement is composed of two assertions stating, respectively, *1)* who can access the resource (Trainers of the `Teaching Quality Evaluation` group) and *2)* the kind of resources involved (SMIL presentations including a video that show trainers instructing trainees). Such assertions are used to

[3]To the benefit of exposition, we keep the example as simple as possible.

define the target of the XACML rule as illustrated in Figure 2. Consider now a request to see presentation `presentation7318.smi` submitted by a user who presents to our system subject metadata stating that the requester is `Sam`, an instructor trainer of the `Teaching Quality Evaluation` Department. Suppose now that according to the hierarchical organization of the concepts defined in the domain ontologies, there is the subsumption: "`Instructor` is a sub-class of `Trainer`". Intuitively, according to this subsumption, the evaluation of the access request should return a permit decision because both `Sam` and the presentation involved in the request satisfy the subject and resource conditions specified in the rule, respectively.

We will see in more details the policy evaluation process in the next Section.

3. POLICY EVALUATION

When a policy involving metadata needs to be evaluated, the subject context already contains the RDF description of the requester, taken from the SAML request. Our policy evaluation engine works as follows.

First, the semantic assertions about the requester that are included in the subject field of our policy rules and the metadata about the requester in the access request are compared to identify the policy rules that apply to the requester. Second, the semantic assertions that are included in the resource context of applicable policy rules are used to query the descriptive metadata of the requested resource, to verify whether the requested resource satisfies the rules selected in the previous step.

Both these selection steps involve RDF queries, where the assertions in the policy rules are used to query metadata associated with the requester and the involved resource. Such querying can be tackled by means of two different techniques: *reasoning* based on metadata and *database-like* querying. The former approach considers RDF metadata as a knowledge base that can be translated into logic programming clauses and applies reasoning techniques to them. Standard Prolog provides a rich processing model which naturally subsumes RDF data. Also, there is a lot of experience implementing in Prolog a variety of alternative processing models (both forward and backward chaining deduction systems, for example).[4] For the latter approach, a suitable query language is DQL, the logic-based query language for the semantic web proposed in [5]. For the sake of clarity here we follow an SQL-like or an XQuery approach, assuming that RDF metadata about resources are stored as a relational or an XML database.

[4] Readers should note that Prolog supports mechanisms for building expressive notations and even languages for knowledge description, which could hide the less friendly aspects of RDF. Ironically, the lack of standardization of Prolog-based notation discourages using it within policies instead of RDF.

```
<?xml version="1.0" encoding="UTF-8"?>
<Rule
  xmlns="urn:oasis:names:tc:xacml:1.0:policy"
  xmlns:xsi= http://www.w3.org/2001/XMLSchema-instance
  xmlns:ctx="urn:oasis:names:tc:xacml:1.0:context"
  xmlns:rdf="http://www.w3.org/TR/WD-rdf-syntax#"
  xmlns:md="http://ourdomain.it/MD/Schema/md-syntax"
  xmlns:ms="http://ourdomain.it/MS/Schema/ms-syntax"
  RuleId="urn:oasis:names:tc:xacml:examples:ruleid:1"
  Effect="Permit">
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch
          MatchId= "urn:ourdomain:function:metadataQuery">
          <AttributeValue
            DataType="http://">
            <rdf:Statement rdf:about="thisRequestUser" >
               <rdf:subject rdf:resource="http://ourdomain.it/MS/Schema/ms-syntax#Trainer" />
               <rdf:predicate rdf:resource="http://ourdomain.it/MS/Schema/ms-syntax#belongs"/>
               <rdf:object rdf:datatype="http://www.w3.org/2001/XMLSchema#string">
                    Teaching Quality Evaluation
               </rdf:object>
            </rdf:Statement>
          </AttributeValue>
        <SubjectAttributeDesignator
          AttributeId="urn:ourdomain:attribute:metatag"
          DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </SubjectMatch>
      </Subject>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatch
          MatchId="urn:ourdomain:function:metadataQuery">
          <AttributeValue
            DataType="http://">
            <rdf:Statement rdf:about="thisRequestUrl">
               <rdf:subject rdf:resource="http://ourdomain.it/MS/Schema/md-syntax#PresSMIL"/>
               <rdf:predicate rdf:resource="http://ourdomain.it/MD/Schema/md-syntax#contains.video"/>
               <rdf:object rdf:nodeID="content"/>
            </rdf:Statement>
            <rdf:Statement rdf:nodeID="content">
               <rdf:subject rdf:resource="http://ourdomain.it/MS/Schema/ms-syntax#Trainer"/>
               <rdf:predicate rdf:resource="http://ourdomain.it/MS/Schema/ms-syntax#instructs"/>
               <rdf:object rdf:datatype="http://www.w3.org/2001/XMLSchema#string">
                    Trainee
               </rdf:object>
            </rdf:Statement>
          </AttributeValue>
        <ResourceAttributeDesignator
          AttributeId="urn:ourdomain:attribute:metatag"
          DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ResourceMatch>
      </Resource>
    </Resources>
    <Actions>
      <Action>
        <AnyAction />
      </Action>
    </Actions>
  </Target>
</Rule>
```

Figure 2. An example of access control policy in extended XACML

First, let us examine the rule selection step. Suppose a request comes in whose encapsulated metadata are:

```
(A, type, statement)
(A, subject, thisRequestUser)
(A, predicate, type)
(A, object, Trainer)
```

Then all XACML rules R whose subject metadata include `(?, subject, Trainer)` (or its subtypes `(?, subject, Instructor)`) will be selected. Let us assume that the resource metadata mentioned in the context of the policy rule R is the following:

```
(?, type, Statement)
```

```
(?, subject, PresSMIL)
(?, predicate, contains_Video)
(?, object, Video)
```

These metadata can now be used to build a query on the resource descriptors, to identify the objects to which the rule applies (e.g., the policy will apply to the SMIL presentation with the metadata shown in Figure 1). The reified statement contained in the policy is used to construct the query which is submitted to the set of resource descriptors. Therefore, to evaluate the feasibility of our approach, the complexity of RDF query answering must be taken into account.[5]

4. RELATED WORK

Several researchers have recently investigated security within the semantic web for the purpose of either expressing security policies or protecting semantically rich data. As an example of the two, the seminal paper by Timothy Finin and Anupam Joshi [11] argues for an ontology based policy language for defining security requirements and a distributed trust management system as main components of a Semantic Web security framework. More recently, Denker et al. [7] developed security ontologies that allow parties to share a vocabulary to exchange security-related information using a common language; while [21] presented examples of policy languages to specify access restrictions over concepts defined in ontologies. More ambitiously, Kagal et al. [16] describe an infrastructure that puts together standard Public Key Infrastructure (PKI) and Role Based Access Control (RBAC) techniques with a distributed trust management system. Another line of work merging security and semantic web concepts is presented in [24] as an approach for identifying Web inference channels due to ontology-based inference attacks. There, an ontology is used to detect tags appearing in different XML documents that are *ontologically equivalent* (i.e., can be abstracted to the same concept in the ontology), but which have contradictory security classifications. Dimitrakos et al. [8] proposed a policy language as a part of a standardized security layer for the Semantic Web, while Gil and Ratnakar [12] introduce a reputation system for rating information sources. Regarding privacy issues, Kim et al. [19] discusses how the Semantic Web will profoundly affect how personal information is collected and used and demands that privacy mechanisms are incorporated into the Semantic Web architecture stack.

Trust and security issues arising from the Semantic Web have been the subject of many other works [1, 13, 14, 17, 20, 22, 25, 26]. Here we limit ourselves to describing a few examples. Agrawal et. al [1] presented a generalization of

[5] Since query evaluation is often exponential in query size, static optimization of queries is an important research issue in this field.

the approach used by algorithms such as PageRank to address the issues of information quality, relevance, inconsistency and redundancy. The purpose is to estimate a user's belief in statements supplied by any other user. The paper formalizes some of the requirements for such a calculus, and describes a number of possible models for carrying it out. Guha et. al [14] developed a framework of trust and distrust propagation schemes. Finally, Kagal et. al [17] provided semantically rich security and policy annotations for OWL-S service descriptions. In particular, they proposed ontologies and markup to capture security information of web service input and output parameters.

5. CONCLUSIONS

Traditional access control models and languages result limiting for emerging Web applications. Although some recently proposed languages allow the specifications of access control rules with reference to generic attributes or properties of the requestor and the resources, they do not fully exploit the semantic power and reasoning capabilities of emerging web applications. In this paper, we have discussed how a semantics-aware approach can help controlling access to resources on the basis of complex metadata about subjects seeking access (as well as about resources themselves). We have also shown how this expressive power could be be in principle accommodated by proper extensions of available XML-based policy languages, like XACML. While several aspects (including efficient techniques for performing enforcement) are still to be investigated, we expect metadata to play a central role in future access control research.

Acknowledgments

The authors wish to thank Pierangela Samarati for joint work on semantics-aware access control. Thanks are also due to Stefano Paraboschi for his valuable contributions on P2P reputation management. This work was supported in part by the European Union within the PRIME Project in the FP6/IST Programme under contract IST-2002-507591 and by the Italian MIUR within the KIWI and MAPS projects.

References

[1] R. Agrawal, P. Domingos, and M. Richardson. Trust management for the semantic web. In *Proc. of the Second International Semantic Web Conference (ISWC2003),* Sanibel Island FL, October 2003.

[2] E. Damiani, S. De Capitani di Vimercati, C. Fugazza, and P. Samarati. Extending policy languages to the semantic web. In *Proc. of the International Conference on Web Engineering,* Munich, Germany, July 2004.

[3] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati. Managing and sharing servents' reputations in P2P systems. *IEEE Transactions on Data and Knowledge Engineering,* 15(4):840–854, July/August 2003.

[4] E. Damiani, S. De Capitani di Vimercati, and P. Samarati. Managing multiple and dependable identities. *IEEE Internet Computing,* November-December 2003.

[5] DAML query language (DQL), April 2003. http://www.daml.org/2003/04/dql/.

[6] J. Davies, D. Fensel, and F. van Harmelen. *Towards the Semantic Web: Ontology-Driven Knowledge Management.* John Wiley & Sons, Ltd, 2002.

[7] G. Denker, L. Kagal, T. Finin, M. Paolucci, and K. Sycara. Security for DAML web services: Annotation and matchmaking. In *Proc. of the 2nd International Semantic Web Conference (ISWC2003),* Sanibel Island, Florida, USA, October 2003.

[8] T. Dimitrakos, B. Matthews, and J. Bicarregui. Towards security and trust management policies on the web.

[9] eXtensible Access Control Markup Language. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

[10] D. Fensel. *Ontologies: A Silver Bullet for Knowledge Management and Electronic Commerce.* Springer-Verlag, 2003.

[11] T. Finin and A. Joshi. Agents, trust, and information access on the semantic web. *ACM SIGMOD,* 31(4):30–35, December 2002.

[12] Y. Gil and V. Ratnakar. Trusting information sources one citizen at a time. In *Proc. of the First International Semantic Web Conference,* June 2002.

[13] J. Golbeck, B. Parsia, and J. Hendler. Trust networks on the semantic web. In *Proc. of the Cooperative Intelligent Agents,* Helsinki, Finland, 2003.

[14] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins. Propagation of trust and distrust. In *Proc. ofthe World Wide Web Conference,* New York, USA, May 2004.

[15] C. Gutierrez, C. Hurtado, and A. Mendelzon. Formal aspects of querying RDF databases. In *Proc. of First International Workshop on Semantic Web and Databases,* Berlin, Germany, September 2003.

[16] L. Kagal, T. Finin, and A. Joshi. A policy based approach to security for the semantic web. In *Proc. of the Second International Semantic Web Conference (ISWC2003),* Sanibel Island FL, October 2003.

[17] L. Kagal, M. Paolucci, N. Srinivasan, G. Denker, T. Finin, and K. Sycara. Authorization and privacy for semantic web services. In *Proc. of the First International Semantic Web Services Symposium, AAAI 2004 Spring Symposium,* March 2004.

[18] R. Khosla, E. Damiani, and W. Grosky. *Human-centered E-business.* Kluwer Academic Publisher, 2003.

[19] A. Kim, L.J. Hoffman, and C.D. Martin. Building privacy into the semantic web: An ontology needed now. In *Proc. of the International Workshop on the Semantic Web Workshop,* Honolulu, Hawaii, May 2002.

[20] M. Marchiori. W5: The five w's of the world wide web. In *Proc. of the Second International Conference on Trust Management,* Oxford, UK, March/April 2004.

[21] L. Qin and V. Atluri. Concept-level access control for the semantic web. In *Proc. of the ACM Workshop on XML Security 2003,* Fairfax, VA, PA, October 2003.

[22] P. Ruth, D. Xu, B. Bhargava, and F. Regnier. E-notebook middleware for accountability and reputation based trust in distributed data sharing communities. In *Proc. of the Second International Conference on Trust Management,* Oxford, UK, March/April 2004.

[23] Security assertion markup language (SAML) v1.0. http://www.oasis-open.org/committees/download.php/3400/oasis-sstc-saml-1.1-pdf-xsd.zip.

[24] A. Stoica and C. Farkas. Ontology guided security engine. *Journal of Intelligent Information Systems,* 2004.

[25] G. Tonti, J.M. Bradshaw, R. Jeffers, R. Montanari, N. Suri, and A. Uszok. Semantic web languages for policy representation and reasoning: A comparison of kaos, rei, and ponder. In *Proc. of the Second International Semantic Web Conference (ISWC2003),* Sanibel Island FL, October 2003.

[26] A. Turner, A. Dorgac, and I. Toroslu. A semantic-based privacy framework for web services. In *Proc. of the Workshop on E-Services and the Semantic Web,* Budapest, Hungary, May 2003.

[27] World Wide Web. *RDF Vocabulary Description Language 1.0: RDF Schema,* December 2003. http://www.w3 .org/TR/rdf-schema/.

[28] World Wide Web Consortium. *Semantic Web.* http://www.w3.org/2001/sw/.