A Comparison of Terminological and Rule-based Policy Languages

Piero A. Bonatti

Università di Napoli Federico II

Security and privacy policies commonly consist of declarative constraints over resource usage (data and services). Therefore logic-based representation languages are well-suited as a foundation of policy languages. Indeed, the semantics of standard languages like XACML can be reformulated in a logic-based fashion similar to the encoding adopted in [2]; moreover, both description logics and logic programming languages (i.e., the two main families of knowledge representation formalisms) have been proposed as policy languages, see KAOS, [7], REI [5], RT [6], Cassandra [1], PeerTrust [4], and PROTUNE [3] just to name a few approaches.

Policy-related processing involves several different reasoning tasks over the axioms that constitute a policy:

- An authorization A is granted iff A is *entailed* by the policy;
- In trust negotiation, a set of credentials C unlocks a resource R iff C and the policy together entail the authorization to use R; the process of finding the sets C that enjoy this property (given the desired authorization for R) is called *abduction*;
- Usability, awareness, and validation issues make it very important to support *explanation facilities* such as those supplied by expert systems; explanation facilities convert axioms and proofs into natural language text understandable by people with no specific training in knowledge representation or computer science; when such documentation is produced automatically, it is guaranteed to be always aligned with the policy actually applied by the system; moreover, automated explanation facilities can produce *contextualized* documentation, relative to specific transactions;
- A natural privacy-related operation is *comparing* the privacy policy published by a web site with the privacy preferences of a user; the relevant question here is whether the information disclosures permitted by the web site's policy will always be permitted also by the user's privacy policy. Policy comparison can also be useful in assessing the results of a policy update; it can answer the question of whether the new policy is more permissive or more restricted than the old one.

In this talk we will assess different knowledge representation formalisms as policy languages for security and privacy, taking into account not only the kind of

constraints that they can express on resource usage, but also the degree to which the above reasoning tasks can be supported. We will conclude that currently rule-based languages are more mature than description logics as far as the general needs of security and privacy policy languages are concerned.

References

1. Moritz Y. Becker and Peter Sewell. Cassandra: Distributed access control policies with tunable expressiveness. In *5th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2004)*, pages 159–168, Yorktown Heights, NY, USA, June 2004. IEEE Computer Society.
2. Piero Bonatti, Sabrina De Capitani di Vimercati, and Pierangela Samarati. An algebra for composing access control policies. *ACM Trans. Inf. Syst. Secur.*, 5(1):1–35, 2002.
3. Piero A. Bonatti and Daniel Olmedilla. Driving and monitoring provisional trust negotiation with metapolicies. In *6th IEEE Policies for Distributed Systems and Networks (POLICY 2005)*, pages 14–23, Stockholm, Sweden, June 2005. IEEE Computer Society.
4. Rita Gavriloaie, Wolfgang Nejdl, Daniel Olmedilla, Kent E. Seamons, and Marianne Winslett. No registration needed: How to use declarative policies and negotiation to access sensitive resources on the semantic web. In *1st European Semantic Web Symposium (ESWS 2004)*, volume 3053 of *Lecture Notes in Computer Science*, pages 342–356, Heraklion, Crete, Greece, May 2004. Springer.
5. Lalana Kagal, Timothy W. Finin, and Anupam Joshi. A policy language for a pervasive computing environment. In *Policies for Distributed Systems and Networks, 2003. Proceedings. POLICY 2003. IEEE 4th International Workshop on*, pages 63–74. IEEE Computer Society, June 2003.
6. Ninghui Li, John C. Mitchell, and William H. Winsborough. Design of a role-based trust-management framework. In *IEEE Symposium on Security and Privacy*, pages 114–130, 2002.
7. A. Uszok, J. Bradshaw, R. Jeffers, N. Suri, P. Hayes, M. Breedy, L. Bunch, M. Johnson, S. Kulkarni, and J. Lott. Kaos policy and domain services: Toward a description-logic approach to policy representation, deconfliction, and enforcement. In *Policies for Distributed Systems and Networks, 2003. Proceedings. POLICY 2003. IEEE 4th International Workshop on*, pages 93–96. ACM Press, June 2003.