Rewrite Specifications of Access Control Policies in Distributed Environments

Clara Bertolissi[1] and Maribel Fernández[2]

[1]LIF, Université de Provence, Marseille, France
[2]King's College London, Dept. of Computer Science, London WC2R 2LS, U.K.
Clara.Bertolissi@lif.univ-mrs.fr, Maribel.Fernandez@kcl.ac.uk

Abstract. In this paper we describe a *metamodel* for access control designed to take into account the requirements of *distributed* environments, where resources and access control policies may be distributed across several sites. This distributed metamodel is an extension of the *category*-based metamodel proposed in previous work, from which standard access control models (e.g. Mandatory and Discretionary access control, Role-based access control, Event-based access control, etc.) can be derived. The metamodel identifies essential notions that are common to access control models, such as categorisation of entities, methods for describing their properties and means for specifying permissions and authorisations. Having a unified common semantics is very important in access control policies where information needs to be shared, as in many distributed applications. We use a *declarative formalism* in order to give an *operational semantics* to the distributed metamodel. We then show how properties of policies can be directly determined from standard results for the operational semantics of access request evaluation.
Key Words: Security Policies, Distributed Access Control, Operational Semantics, Rewriting

1 Introduction and Background

The generalisation of the use of access control policies in distributed computing environments has increased the need for high-level declarative languages that enable security administrators to specify a wide range of complex policies. Moreover, given the complexities and scope involved, distributed applications have increased the requirements for autonomously changing policies (they require dynamic and/or location-dependent policies).

Using a formal specification for defining access control models and policies is particularly important in distributed contexts. The first attempts to develop formal theories to define and validate security policies (see, for instance, [8]) have used first-order theorem provers, purpose-built logics, or flow-analysis, but these approaches have limitations (as discussed for instance in [19]). More recently, rewriting techniques have been fruitfully exploited in the context of security protocols (see [3]), security policies controlling information leakage (see [14]), and access control policies (see [20, 6]). Along these lines, rewriting tools appear

to be very well adapted for providing a semantics for distributed access control mechanisms. On one hand, security policies and protocols can conveniently be specified as sets of rules, which can be formalised as a rewriting system (for instance the Needham-Schroeder public key protocol, and policies for control of information leakage, have been specified as rewrite systems [1, 14]). On the other hand, rewrite systems provide a multiparadigm computation model: they have been used as a semantics for logic programming languages (via unification and narrowing [15]), for functional languages (via matching and reduction [17, 10, 11]) and they can express imperative and concurrent features (in-place update [13], or a process calculus [18]). Thus, a rewrite-based framework with access control mechanisms can be used to derive distributed logic, functional or imperative programming languages. Moreover, the possibility to write policies as sets of authorisation rules offers administrators more flexibility and simplicity for writing and composing access control policies.

Over the last few years, a variety of access control models and languages for access control policy specification have been developed, often motivated by particular applications. We can mention the ANSI (hierarchical) role-based access control (H-RBAC) model [16], further extended with time and location constraints [9], the mandatory access control (MAC) model [4], the event-based access control (DEBAC) model [6], etc. A unifying metamodel for access control, which can be specialised for domain-specific applications, has been recently proposed in [2]. This approach has advantages: for example, by identifying a core set of principles of access control, one can abstract away many of the complexities that are found in specific access control models; this, in turn, helps to simplify the task of policy writing. A rewrite-based operational semantics for this metamodel was described in [7], where the expressive power of the metamodel is also demonstrated by showing that the above mentioned access control models can be derived as specific instances of the metamodel.

2 Contributions and Motivations

Based on the work in [7], in this paper we define a category-based access control metamodel for *distributed environments*, and provide a formal specification of access control evaluation using a declarative framework.

A key aspect of our approach, following [2], is to focus attention on the notion of a *category*. A category (a term which can, loosely speaking, be interpreted as being synonymous with, for example, a sort, a class, a division, a domain) is any of several fundamental and distinct classes to which entities or concepts belong. We regard categories as a primitive concept and we view classic types of groupings used in access control, like a role, a security clearance, a discrete measure of trust, etc., as particular instances of the more general notion of category.

Here we will adapt the idea of categorisation to a distributed setting, extending the work reported in [7]. In a system with dispersed resources, classifications of entities may depend on the site to which the entity belongs. Moreover, per-

missions associated to categories of entities can refer locally to the site where the category is defined. Therefore, we may want to use a distributed access control evaluation method, in addition to the central one proposed in [7], or we may want to combine the two. An algebraic functional framework for distributed access control which permits the definition of centralised or distributed access evaluation mechanisms has been proposed by the authors in [5] in the particular case of the event-based access control model DEBAC. We will show in this paper that the techniques introduced in [5] can be adapted in order to extend the category-based metamodel.

In the full paper, after recalling the background material on access control models and term rewriting, we define the extension of the category-based metamodel to deal in a uniform way with distributed systems where different access control policies are maintained locally. We will then show that Distributed DEBAC can be derived as an instance of the distributed metamodel. Finally, we show how properties of access control policies can be derived from standard properties of the rewrite framework we use.

The rewrite-based specification that we describe enables access control policies to be defined in a declarative way and permits properties of access control policies to be proven. Rule-based policy specifications have the advantage to be concise, easy to maintain for security administrators, and easy to share with users. Those advantages are in great part due to the high level of abstraction of the languages used. Using rule-based languages in this setting ensures in particular an improved expressiveness and clean and unambiguous semantics. Moreover, the declarative nature of this kind of policy specifications enhance modularity, which is a crucial aspect when considering distributed security policies developed independently by different departments, organisations or institutions. Rewriting systems present many advantages as a specification tool: they have a well-studied theory, with a wealth of results that can be applied to the analysis of policies, and several rewrite-based programming languages are available (see, e.g., Maude [12]).

Summarising, the main contributions of this paper are:

- a declarative, rewrite-based specification of a distributed access control metamodel (extending [7] to incorporate the notion of site and policies distributed across several sites);
- a formal operational semantics for access request evaluation, in centralised as well as in distributed contexts where information is shared.
- the definition of Distributed-DEBAC as an instance of the distributed metamodel, to demonstrate the expressive power of the metamodel.
- a technique to prove totality and consistency of access control policies, by proving termination and confluence of the underlying term rewriting system.

References

1. A. Armando, L. Compagna, and Y. Lieler. Automatic compilation of protocol insecurity problems into logic programming. In *Proc. JELIA'04*, volume 3229 of

Lecture Notes in Computer Science, 2004.
2. S. Barker. The next 700 access control models or a unifying meta-model? In *Proc. of SACMAT 2009*, pages 187–196. ACM Press, 2009.
3. G. Barthe, G. Dufay, M. Huisman, and S. Melo de Sousa. Jakarta: a toolset to reason about the JavaCard platform. In *Proc. of e-SMART'01*, volume 2140 of *Lecture Notes in Computer Science*. Springer-Verlag, 2002.
4. D. E. Bell and L. J. LaPadula. Secure computer system: Unified exposition and multics interpretation. *MITRE-2997*, 1976.
5. C. Bertolissi and M. Fernández. An algebraic-functional framework for distributed access control. In *Proc. of Crisis 2008*. IEEEXplore, 2008.
6. C. Bertolissi, M. Fernández, and S. Barker. Dynamic event-based access control as term rewriting. In *Proc. of DBSEC 2007*, volume 4602 of *Lecture Notes in Computer Science*. Springer-Verlag, 2007.
7. C. Bertolissi and M. Fernández. Category-based authorisation models: Operational semantics and expressive power. In *Proc. of ESSoS 2010, Pisa, Italy, 2010*. Volume 5965 of *Lecture Notes in Computer Science*, pages 140–156. Springer, 2010.
8. P. A. Bonatti and P. Samarati. Logics for authorization and security. In J. Chomicki, R. van der Meyden, and G. Saake, editors, *Logics for Emerging Applications of Databases*, pages 277–323. Springer, 2003.
9. S. M. Chandran and J. B. D. Joshi. *LoT-RBAC*: A location and time-based rbac model. In *WISE 2005, NY, USA, Proceedings*, volume 3806 of *Lecture Notes in Computer Science*, pages 361–375. Springer, 2005.
10. H. Cirstea and C. Kirchner. The Rewriting Calculus - Part I. *Logic Journal of the Interest Group in Pure and Applied Logics*, 9:363–399, May 2001.
11. H. Cirstea and C. Kirchner. The Rewriting Calculus - Part II. *Logic Journal of the Interest Group in Pure and Applied Logics*, 9:401–434, May 2001.
12. M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Martí-Oliet, J. Meseguer, and C. Talcott. The Maude 2.0 system. In Proc. of *RTA 2003*, number 2706 in *Lecture Notes in Computer Science*, pages 76–87. Springer-Verlag, 2003.
13. D. Dougherty, P. Lescanne, L. Liquori, and F. Lang. Addressed term rewriting systems: Syntax, semantics and pragmatics. In *Proc. of TERMGRAPH'04*, ENTCS. Volume 127, Issue 5, Pages 57-82. Elsevier, 2005.
14. R. Echahed and F. Prost. Security policy in a declarative style. In *Proc. of PPDP'05*. ACM Press, 2005.
15. M. Fernández. Narrowing based procedures for equational disunification. *Applicable Algebra in Engineering, Communication and Computing*, 3:1–26, 1992.
16. D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli. Proposed NIST standard for role-based access control. ACM Trans. Inf. Syst. Secur. Volume 4(3), pages 224–274, 2001.
17. J. Goguen, T. Winkler, J. Meseguer, K. Futatsugi, and J-P. Jouannaud. Introducing obj. In G. Malcolm, editor, *Software Engineering with OBJ: algebraic specification in action*. Kluwer, 2000.
18. M. Hennessy, J. Rathke, and N. Yoshida. Safedpi: A language for controlling mobile code. Journal of ACM Acta Informatica. Volume 42(4), pages 227-290. Springer-Verlag, 2005.
19. R. Jagadeesan and V. Saraswat. Timed Constraint Programming: A Declarative Approach to Usage Control. In *Proc. of PPDP'05*. ACM Press, 2005.
20. A. Santana de Oliveira. *Réécriture et modularité pour les politiques de sécurité*. Thèse de doctorat, Université Nancy 1, 2008.