Journal of Visual Languages and Computing 21 (2010) 41–64

Contents lists available at ScienceDirect

Journal of Visual Languages and Computing

journal homepage: www.elsevier.com/locate/jvlc

A system for visual role-based policy modelling

Massimiliano Giordano [a], Giuseppe Polese [a], Giuseppe Scanniello [b,*], Genoveffa Tortora [a]

[a] Dipartimento di Matematica e Informatica, University of Salerno, Via Ponte Don Melillo, 84084 Fisciano (SA), Italy
[b] Dipartimento di Matematica e Informatica, University of Basilicata, Viale Dell'Ateneo 10, Macchia Romana, 85100 Potenza, Italy

ARTICLE INFO

Article history:
Received 29 December 2008
Received in revised form
25 September 2009
Accepted 20 November 2009

Keywords:
RBAC
Role-based security policy
Visual languages
XACML
Eclipse IDE

ABSTRACT

The definition of security policies in information systems and programming applications is often accomplished through traditional low level languages that are difficult to use. This is a remarkable drawback if we consider that security policies are often specified and maintained by top level enterprise managers who would probably prefer to use simplified, metaphor oriented policy management tools.

To support all the different kinds of users we propose a suite of visual languages to specify access and security policies according to the role based access control (RBAC) model. Moreover, a system implementing the proposed visual languages is proposed. The system provides a set of tools to enable a user to visually edit security policies and to successively translate them into (eXtensible Access Control Markup Language) code, which can be managed by a Policy Based Management System supporting such policy language.

The system and the visual approach have been assessed by means of usability studies and of several case studies. The one presented in this paper regards the configuration of access policies for a multimedia content management platform providing video streaming services also accessible through mobile devices.

1. Introduction

Large and modern organizations need to handle a huge number of access rules and constraints for guaranteeing secure access to sensitive data within their information systems. They need security paradigms that can be easily understood and managed by enterprise managers, because they are the ones who have the knowledge about the enterprise and the way its resources should be accessed. To this end, different access models have been proposed, such as discretionary access controls [1], mandatory access controls [2], access control list [3], task based authorization [4], and the role-based [5,6]. They require the enterprise manager to have specific knowledge in order to be able to define access control policies based on request/response scenarios.

In the role-based access control (RBAC) model the policies relate information on users, resources, applications, security characteristics, factory priorities, and network features [7]. They describe the kind of user that can benefit from a given application, the priority in using it, and finally the network resources allocatable for that application. For example, priorities in using bandwidth might have to be defined for a company, whose employees need to access internet for visiting a Web site or for a crucial activity in a workflow. RBAC is particularly suitable to model policies in which the privileges to use a resource are connected to a role rather than to a specific user. Each user can belong to more than one role, and for each of them several privileges can be defined. When an employee changes its position in the organization chart, the manager assigns him/her a new role discarding the old one.

* Corresponding author.
E-mail addresses: mgiordano@unisa.it (M. Giordano), gpolese@unisa.it (G. Polese), giuseppe.scanniello@unibas.it (G. Scanniello), gtortora@unisa.it (G. Tortora).

1045-926X/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jvlc.2009.11.002

RBAC policies can be defined by using several access control languages. One of the most frequently used standardized language for defining policies is XACML (eXtensible Access Control Markup Language) [8], an XML based language to define actions and rules for subjects and targets. XACML defines two types of languages for modelling both control policies and request/response on resources. The first type of language is used to express access control policies, specifying who can make what, where, and when. The second type of language is used to define queries on whether a particular access should be allowed (requests), and to describe answers to such queries (responses), such as Permit, Deny, Indeterminate, and Not Applicable.

Although XACML provides a powerful abstraction for policy definition in heterogeneous frameworks, tools assisting administrators in the management of policies are highly desirable. Visual language based policy management systems should enable the high level specification and management of access policies. They introduce a further level of abstraction with respect to XACML, enabling the modelling of policies according to metaphors close to the specific application domain and to human reasoning. Thus, they can considerably simplify the work of enterprise security managers.

In this work we propose a visual language based system for specifying role based access policies and for implementing them in the XACML language. In particular, we describe a suite of visual languages enabling the management of role-based access policies [5,6] in heterogeneous frameworks and configurable networks, providing a metaphor oriented layer above the RBAC model. Moreover, the approach can be proficiently embedded within software engineering methodologies to specify access policies to be enforced during the design of information systems and applications.

The main visual language in our proposal is the Role Diagram, which is used to specify roles. It allows us to model roles and relations among them. Access policies are defined through the Permission Diagram, which allows an administrator to specify who can use the available resources. Constraints are described through the Separation of Duties Diagram. It is used to specify resources that cannot be employed by users who have played a given role, which must have been previously defined in the Role Diagram. Finally, in order to assign users to roles we propose the Role Assignment Diagram.

This set of visual languages has been embedded within a system providing editors to compose visual sentences and compilers to generate access policies abiding by the XACML standard. The system also includes a server for policy management and access request evaluation, and a development environment supporting policy design, which has been implemented as an *Ecplise* plug-in. The system has been used experimentally in several case studies. The one described in this paper regards the configuration of access policies for a multimedia content management platform providing video streaming services accessible through several types of devices, including mobile devices. We have previously used the system in the context of collaborative environments, and in Voice Over Ip infrastructures. We are currently using it in the context of domotics applications. A controlled experiment to compare our tool and the one of the most pertinent competitor, namely XGrid Tool, has been also conducted and the results have been presented and discussed as well.

The remainder of the paper is organized as follows. Section 2 briefly presents some concepts concerning visual languages, RBAC, and XACML. The proposed visual languages are detailed in Section 3, whereas the system prototype is illustrated in Section 4. The case study and system usability issues are discussed in Sections 5 and 6, respectively. In Section 7 we present the comparative evaluation between our tool and XGrid Tool which also uses a visual based approach. Related works are discussed in Section 8. Finally, discussion is provided in Section 9.

2. Background

In this section we briefly recall some basic concepts underlying the proposed system. These include visual languages, the role based access control model, and the eXtensible Access Control Markup Language.

2.1. Visual languages

Visual and diagrammatic representations play a central role in several application domains [9,10], since they provide important tools for describing and reasoning. As visual languages have been applied to new application domains, such as spatial databases, education, software engineering, and so forth, many different types of visual notations and underlying grammar models have been devised. As for visual language grammars, many different formalisms have been proposed in the literature [9]. Since in the rest of the paper we will describe several visual languages and will show how to model them through one of such formalisms, namely the Extended Positional Grammars (XPGs), in the following we will review the basic concepts underlying XPGs.

XPGs represent a direct extension of context-free string grammars. In particular, the XPG formalism is based on an extension of LR (Left to Right) parsing named XpLR (eXtended Positional Left to Right) methodology [11]. The XPG formalism conceives a sentence as a set of symbols with attributes. Such attributes can be classified in physic, syntactic, and semantic attributes. The physical component represents the features of a symbol and allows us to materialize the sentence to our senses; whereas the values of the syntactic attributes are determined by the relationships holding among the symbols. Thus, a sentence is specified by combining symbols with relations.

More formally, an Extended Positional Grammar is the pair (G, PE), where PE is a *positional evaluator*, and G is a particular type of context-free string attributed grammar $(N, T \cup POS, S, P)$ where:

- N is a finite non-empty set of *non-terminal* symbols;
- T is a finite non-empty set of *terminal* symbols, with $N \cap T = \emptyset$;