Information Sciences 179 (2009) 2629–2642

Contents lists available at ScienceDirect

Information Sciences

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

Specification and enforcement of flexible security policy for active cooperation ☆

Yuqing Sun [a,*], Bin Gong [a], Xiangxu Meng [a], Zongkai Lin [c], Elisa Bertino [b]

[a] School of Computer Science and Technology, Shandong University, No. 27 Shanda South Road, Jinan Shandong 250100, China
[b] CERIAS and Department of Computer Science, Purdue University, USA
[c] Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China

ARTICLE INFO

Article history:
Received 1 August 2007
Received in revised form 29 May 2008

Keywords:
Security policy
Access control
Flexibility
Cooperation
RBAC

ABSTRACT

Interoperation and services sharing among different systems are becoming new paradigms for enterprise collaboration. To keep ahead in strong competition environments, an enterprise should provide flexible and comprehensive services to partners and support active collaborations with partners and customers. Achieving such goals requires enterprises to specify and enforce flexible security policies for their information systems. Although the area of access control has been widely investigated, current approaches still do not support flexible security policies able to account for different weighs that typically characterize the various attributes of the requesting parties and transactions and reflect the access control criteria that are relevant for the enterprise. In this paper we propose a novel approach that addresses such flexibility requirements while at the same time reducing the complexity of security management. To support flexible policy specification, we define the notion of restraint rules for authorization management processes and introduce the concept of impact weight for the conditions in these restraint rules. We also introduce a new data structure for the encoding of the condition tree as well as the corresponding algorithm for efficiently evaluating conditions. Furthermore, we present a system architecture that implements above approach and supports interoperation among heterogeneous platforms.

1. Introduction and motivation

Today enterprises heavily rely on information systems and applications. As a result many tasks that in the past were carried by humans are today automatically executed by computer systems. As a consequence sharing, interoperating and combining services across multiple enterprises are today easier. To keep ahead in strong competition environments, enterprises should provide flexible and comprehensive services to partners and support active collaborations with partners and customers. Achieving such goals requires the development of novel access control models and mechanisms able to address the following requirements.

Flexible specification of access control policies: Consider a scenario of supply chain management, and suppose that an enterprise would grant different access rights to sensitive information to partners according to their qualifications, relationships

☆ Research supported in part by the National High Technology Research and Development Program (863 Program) of China (2006AA01A113), by the US NSF Grant 0712846 “IPS: Security Services for Healthcare Applications”, by the NSF grant of Shandong Province of China (Y2008G28), and by the sponsor of CERIAS.

* Corresponding author. Address: School of Computer Science and Technology, Shandong University, No. 27 Shanda South Road, Jinan Shandong 250100, China.

E-mail addresses: sun_yuqing@sdu.edu.cn (Y. Sun), gb@sdu.edu.cn (B. Gong), mxx@sdu.edu.cn (X. Meng), lzk@ict.ac.cn (Z. Lin), bertino@cs.purdue.edu (E. Bertino).

0020-0255/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2009.01.040

or transaction contents. For example, a medical instrument manufacturer would like to grant the permission for accessing detailed information from its latest database to a VIP partner, while would like to grant a browsing permission to summary information to a generic partner. Such flexible access control policies require to perform access control by taking into account a comprehensive set of information about the requesting partner. In such process, each information item may have a different importance. For example, the enterprise may consider more relevant the certification granted by a trusted national organization compared with history transaction. Thus a greater weight should be assigned to certification while a smaller weight should be assigned to history transaction. Policies are also characterized by a temporal dimension and therefore historical data should also be taken into account in access control. We would like to associate different weights with data from different temporal periods in order to reflect temporal criteria, such as that more recent data have greater weights.

Flexible enforcement of access control policies: It is increasingly important to take into account environment factors when enforcing access control policies. To address such requirement an access control mechanism should dynamically monitor state changes of the underlying system and take into account such changes in the policy enforcement process [1,14]. For example, qualifications of a user might be changed by the transactions carried out by the underlying systems; for example the relationship *partner* could be upgraded to *VIP partner* on the assumption that the trade amount exceeds 100 million dollar within one year.

Flexible adaptation of access control policies: To effectively support collaborations, access control policies need to evolve along with the business developments and changes in the enterprise mission. For example, an enterprise may decide to open more sensitive information to partners than in the past, and thus adjust the qualification threshold of *VIP partner* to a lower level 75 million dollar of trade amount.

The above flexibility requirements about access control systems arise not only from industry but also in the military and government domains. Therefore, they are important requirements for the development of access control models and mechanisms to be used in collaborative applications.

Although widely used access control models, like DAC (Discretionary Access Control), MAC (Mandatory Access Control) and RBAC (Role Based Access Control) [7], are appropriate for conventional database and application environments, they do not meet the above requirements. In most cases, they are based on predefined regulations; if changes are required, the access control policies must be manually adjusted which is time consuming and error-prone. When a system supports a large amount of users, characterized by a large diversity of factors, upgrading the access control policies quickly becomes an impossible task.

Recently, extensions to conventional access control models have been proposed to support advanced applications. Examples of such extensions include content-aware access control, user qualification based authorization management, and attribute based access control (ABAC) [2,6,22]. Despite their advantages, they are still not able to support more active security policies, in particular because they do not take into account data transactions. Rule-based access control, like rule-based user-role assignment, is also considered an effective method to support flexible enforcement of access control policies. However, it does not take into account the important requirement that different weights may have to be assigned to the various attributes, characterizing the parties requesting access, nor the fact that authorizations may have to change as consequence of transactions executed by these parties.

In this paper we propose a novel approach that addresses the above flexibility requirements, while at the same time reducing the complexity of security management. Our approach focuses on the specification and enforcement of flexible access control policies, by taking into account the underlying transactions, user attributes, and application context when making access control decisions. Our approach is based on the notion of *restraint rules* which are associated with authorization management processes. We also introduce the concept of *impact weight*; this weight is associated with the condition of each restraint rule. To efficiently enforce such rules, we introduce a new data structure, referred to as *condition tree*, as well as corresponding algorithms to evaluate rule conditions. Furthermore, we also present a system architecture that implements the proposed approach and is able to support interoperation among heterogeneous platforms.

The remainder of this paper is organized as follows. Next section discusses related work. The proposed model is introduced in Section 3. Section 4 discusses the calculation of restraint rules. The subsequent sections present a comprehensive example to illustrate our approach and an overview of the system architecture, respectively. The final section outlines conclusions and future work.

2. Related work

RBAC is a widely adopted access control model to secure resources in an information system [17]. In RBAC, permissions are associated with roles, and users acquire permissions by being assigned roles. Roles within an organization typically have overlapping sets of permissions and thus they can be organized according to role hierarchies. Constraints are used to reflect security policies of an organization, like Separation of Duty (SoD) that formulates multi-person control policies to discourage frauds. Although RBAC provides a powerful mechanism to secure large systems, manual adjustment of authorizations has to be carried out to reflect policy changes by the enterprise.

Recently, approaches have been proposed to support automatic authorization management [9]. AI-Kahtani et al. propose a family of models, called RB-RBAC, to support automatic user-role assignments based on user attributes and a set of authorization rules [3,4]. The central features of RBAC such as roles, role hierarchies, and constraints can be specified based on user