Challenges of Meta Access Control Model Enforcement to an Increased Interoperability

Sérgio Luís Guerreiro
University of Lisbon, Portugal

INTRODUCTION

Today, countless access control models (ACM) solutions are available in the academy and industry. Nevertheless, the recognized development of ACM, in the majority of situations, these solutions specifies and implements the structural security access concerns of a single organizational silo (Sandhu *et al.*, 2000). Typically, ACM solutions are designed to fit and follow policies that are applied to a specific application layer of an organization. Early examples of such approach are the discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), time-role-based access control (TRBAC), Orcon or Chinese wall (Ferraiolo *et al.*, 2001; 2007).

Following this problem, Ferraiolo & Alturi (2008) raise the discussion about the feasibility of designing a meta access control model (MACM) fitting any specific ACM. So far, there are no bibliographic proofs that solve this posed problem. Moreover, Baker (2009) contributes to this discussion, stating the need to define a meta-ACM rather than specifying multiple instances in order to minimize the duplication of effort. Accordingly, to this author, the first goal to achieve in this endeavor is ACM conceptualization, and exemplifies it stating that RBAC is a particular instance of a MACM.

Moreover, recent advances proposed by Korman *et al.* (2016) show that the myriad of ACM solutions available difficult the management of IT models. Therefore, these authors propose an ACM meta-model, designed in ArchiMate (The Open Group, 2013) to be used by the Enterprise Architects professionals. The meta-model is derived from the conceptual mapping of seventeen different ACM models. Then, ArchiMate relates the meta-model with enterprise concepts. In the end a unified meta-model for modeling authorization within enterprises is presented.

One the other hand, from a first sight, positioned in a different scientific field, interoperability is referred by Naudet *et al.* (2008) as "interoperability problem appears when two or more incompatible systems are put in relation". In a broader sense, "Interoperability requirement is a statement that specifies a function, ability or characteristic, related to the capacity of a partner to ensure its partnership regarding compatibility, interoperation, autonomy, and reversibility, which it must satisfy" (Mallek *et al.*, 2012). Therefore, interoperability is considered as a key capacity to partners' cooperation success (Patil *et al.*, 2007; Reul *et al.*, 2010). However, when two or more systems are interoperating, most of times, different ACM are in place and a barrier to the interoperation appears.

Therefore, given the context of ACM and interoperability, the following research question is logically raised: How to design and enforce a meta-access control model to facilitate the interoperability between different access control mechanisms?

For short, this paper assesses the possibility of using a meta-access control model to conceptual-

DOI: 10.4018/978-1-5225-2255-3.ch056

ize and instantiate many access control models. In specific, this research explores the following challenges:

- **Access Models Interoperability:** The paper uses a MACM to abstract all the concepts and relations contained in the many ACMs, and therefore creating interoperability between them.
- **Standardization of Storage for Access Data:** Standardization is realized through a single repository (and unique) for the MACM. When needed the MACM is instantiated for a specific ACM.
- **Provisioning of Access Models:** The MACM and ACM relationship enables the dynamic creation, reading, updating and deleting of access models, in order to adapt to the evolving organizational access requirements.

This paper has two-fold contributions: technological and societal. On the one hand, technological benefits are identified because of easier ACM implementation in each organization. On the other hand, societal benefits are related with lowering financial investments to interoperate the different organizations (*e.g.*: adaptive software enterprise resource planning (ERP) solutions between two small or medium enterprises).

This paper is organized as follow. Firstly, the research background is presented. Then, meta-access control model (MACM) is formalized. After that, solutions and recommendations are identified for the MACM. Then, future research directions are discussed. Finally, the last section concludes the paper.

BACKGROUND

Generically, a control system offers the capability to react whenever any disturbance affects the behavior of the controlled system or whenever a new reference is established (Guerreiro *et al.*, 2016). Disturbance is assumed whenever the system is not producing the desired output for the imposed input. In these situations, the control system acts in the input, to change the controlled system's state.

Ferraiolo *et al.* (2007) defines that access control systems, or authorization in its broadest sense, is present in today's every information technology and is concerned with the ways in which users can access resources in the computer system, or informally speaking, with ”who can do what”. By these authors, access control is arguably the most fundamental and most pervasive security mechanism in use today. The author compares the actual access control models with the Guards, gates and locks that have been used since the ancient times to limit the individual's access to the valuables.

Nowadays, organizations use access control mechanisms to mitigate the risks of unauthorized access to their data, resources, software systems, etc. Each access request is assessed against a predefined authorization schema, and as a result, the access will be granted or denied. Several access control models exist to address changes in organizational structures, technologies, organizational needs, technical capabilities, and organizational relationships.

The standard NIST98 (Ferraiolo *et al.*, 2001; Sandhu *et al.*, 2000) is the most frequently used. It models the concepts for symmetric role-based access control (RBAC) to be used between the users, roles, permissions and constraints, as represented in Figure 1. It represents an evolution from the Discretionary Access Control (DAC) that grants access of individual object to individuals; Mandatory Access Control (MAC) and other policies due to less provisioning effort needed (Smith, 1997). Other known policies are different flavors of DAC, Time-Role Based Access Control (TRBAC), ORCON or Chinese wall. In RBAC the users are directly assigned to a role, each role has a set of associated permissions and changing the permissions affects the users associated with each role. Some well known constraints are separation of duties (SoD), conflict of interest (CoI), delegation of duties (DoD), binding of duty (BoD), least