Chapter XVI

Adding Context into an Access Control Model for Computer Security Policy

Shangping Ren, Illinois Institute of Technology, USA
Jeffrey J. P. Tsai, University of Illinois at Chicago, USA
Ophir Frieder, Illinois Institute of Technology, USA

Abstract

In this chapter, we present the role-based context constrained access control (RBCC) model. The model integrates contextual constraints specified in first-order logic with the standard role-based access control (RBAC). In the RBCC access control model, the permission assignment functions are constrained by the user’s current accessing contexts. The accessing contexts are further categorized in two classes, that is, system contexts and application contexts. System contexts may contain accessing time, accessing location, and other security-related system information; while application contexts are abstractions of relationships among different types of entities (i.e., subjects, roles, and objects) as well as implicit relationships derived from protected information content and external information. The ability to integrate contextual information allows the RBCC model to be flexible and capable of specifying a variety of complex access policies and providing tight and just-in-time permission activations. A set of medical domain examples will be used to demonstrate the expressiveness of the RBCC model.

Copyright © 2007, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
Introduction

Networked computers reside at the heart of systems on which people now rely, both in critical national infrastructures and in private enterprises. Today, many of these systems are far too vulnerable to cyber-attacks that can inhibit their functioning, corrupt important data, or expose private information. For instance, more and more medical facilities are digitizing their records daily. This trend necessitates security protocols that protect patient privacy and at the same time provide convenient timely access. To provide security constraints, often a role-based access control (RBAC) model-based approach is used. In such an approach, user roles define access rights. However, as we later show, these measures are insufficient in medical applications, and thus, we present the role-based context constrained (RBCC) model that integrates constraints with the traditional RBAC model using first-order logic. In addition to assigning access rights based on roles as in an RBAC approach, context constraints also play an important role in assigning access rights in the RBCC model.

In RBAC based approaches, individuals are associated with roles, and the security policy is based only on roles. In particular, once the individual assumes a role in a given session, the role becomes the only factor in deciding the individual’s access rights, and the individual’s own identity is ignored in such decision process. Hence, the access control in the RBAC model is very coarse-grained and at the role level only.

Unfortunately, in many commercial applications such as the healthcare domain, role level coarse-grained access control is not sufficient to enforce individual-based privacy rules. Consider a security rule: a head nurse is allowed to view all patient medical files if the patient’s doctors are in the same department as the head nurse and the patients are not under the supervision of the head nurse. In this example, although the policy defines access privilege for the head nurse role, a different head nurse in the same department may have a different set of records that he/she can view. More specifically, the user’s identity and the relationship between the user (the head nurse) and the owner of the records (patient’s records) as well as the role decide the access rights. As RBAC only provides coarse-grained and role level control, it is difficult to model such fine-grained security policy if not impossible.

The example has also shown other characteristics of access control in healthcare applications. For instance, the accessing context (such as time, location, relationships among entities) has impact factors in deciding access rights. Unfortunately, such factors are not considered in current RBAC model and existing extension-based solutions.

We present a model that integrates a traditional RBAC model with context constraints. The presented RBCC model can dynamically constrain the role-permission relationship based on the current accessing context. The accessing context may contain current user, role, object, and system properties, relationships among these entities, and implicit external information. With the RBCC model, the traditional static role-permission assignment function in the RBAC model becomes dynamic and state dependent, and hence allows for fine-grained access control.