Article Review

X-GTRBAC: an XML-based policy specification framework and architecture for enterprise-wide access control

by

George Dimitoglou


Appeared: June 7 2006, Computing Reviews, Association of Computing Machinery (ACM), CR132886.

The title of this paper alone is enough to raise questions about whether this is an old solution to an old problem with an Extensible Markup Language (XML) twist, particularly after a simple search in The Collection of Computer Science Bibliographies for the terms access control and framework yields 94,693 results.

Cynicism aside, the work by the authors is excellent. The focus of this paper is on presenting a secure content-based access framework for enterprise resources supporting fine-grained dynamic access control. It is obvious that the authors have done a lot of good work on the topic, and this shows in every aspect of the paper: its structure, the complete examples, and the clarity with which they express their ideas.

The introduction provides enough information to set the stage for the rest of the material relating to access control. It stays at a high level, and gently ushers the reader into the operational environment by describing the basic premises and interactions between policies, resources, and methods of their control.

The title of the second section (Preliminaries) is as true to advertising as it can be. An introduction to XML, with examples, along with a similar examination of the role-based access control (RBAC) model, provides enough information for even the uninitiated to follow. For other readers, the XML introduction can be skipped.

The Motivation and Goals section explains the reasons behind using XML, and the adaptation of the generalized temporal role-based access control (GTRBAC) model. The description of the capabilities that GTRBAC affords, content-based context-aware access and heterogeneity of subjects and objects, is sufficient to justify the selection of the particular model. The outline of the formal specification of the GTRBAC model, immediately after this section, covers all necessary aspects of the model that could be useful when deploying such a role-based access control infrastructure.

The fifth section is the central part of the paper, where the X-GTBRAC specification language is described in detail. The specification seems to be extensive, and flexible enough to accommodate any enterprise resource access control environment. Clearly, one way to test the specification is to build a system and run examples, which is precisely what the authors do in the following sections. The implementation part of the system is prefaced by the system architecture, with a number of diagrams and explanations of the different system interrelations. Multiple examples, with snippets of XML documents, illustrating the definitions of triggers, users, and constraints are provided, making the flow of the paper very smooth, and the content easy to follow.

The Related Work section provides a thorough investigation of prior relevant work, and shows that the material is based on solid scholarly foundations. The Conclusions sections summarizes the work, and provides some ideas for future directions. Overall, this is a very thorough and extensive piece of work, and the existence of much similar work in the area does not discount its contribution in any way. Some of the sections of the paper could have been shortened or omitted altogether, simply because many of the technologies (for example, XML) are an inseparable part of the current
computing landscape, and do not need such detailed coverage. Beyond this superficial observation, the material is well supported, and the examples are succinct and appropriate, and enable the reader to follow the material with great ease.

Hopefully, the authors will continue their work, and be able to address the challenges and opportunities they outlined for distributed inter-enterprise environments and the efficient administration and management of global-level policies.