

On Conceptual Modelling and Design of Role-Based Access Control Systems

Yanchun Zhang

School of Computer Science and Mathematics
Victoria University
PO Box 14428, Melbourne City, MC
VIC 8001 Australia
yzhang@csm.vu.edu.au

Extended Abstract

While conceptual modelling has been prevail in database and information systems design & development, it also plays an important role in many other complex systems design where the relationships among components and elements are complicated and need proper modelling/understanding.

In this talk, we present a formal approach for role-based access control systems design and emphasize the role of conceptual modelling of various relationships and constraints in RBAC systems. Users access control is a critical and sensitive issue in many systems and applications, especially for many web-based systems with large number of users, proper access control is a key issue for system security. Role-based access control governs users' access to the information on the basis of users' positions in the organisation (outside the organisation as well). RBAC involves individual users being associated with roles as well as roles being associated with permissions (Each permission is a pair of object set and operation set). As such, a role is used to associate users and permissions. A user in this model is a human being. A role is a job function or job title within the organization associated with authority and responsibility.

The relationships between users and roles and/or between roles and permissions are complicated by the facts that roles may have hierarchical structures with role inheritance from the junior roles to senior roles, some may conflict with each other due to security reason, user' roles may change during the course, such as further roles can be granted, some roles may be revoked, etc. For example, when granting further roles to a user, the new roles together with the existing roles may enable the user to access or derive some more restricted information of higher level security than he or she is entitled. To maintain the system consistency and security, the complex relationships need to be modelled and automatic algorithms need to be in place to check the consistence

when granting and updating user-role and role-permission assignments.

In this work, we start with conceptual modelling of various relationship and constraints, and introduce formal algebraic notations to specify the constraints, and then develop formal algorithms and procedures to check the conflicts and help administrators to assign and allocate roles to users and permissions to roles.

This work aims at two contributions, (1) develop a formal approach for RBAC system modelling and design, and (2) promote the use and role of conceptual modelling in complex system design.

Keywords: conceptual modelling, integrity constraints, role-based access control, relational algebra