Using Description Logic to Formalize Role-Based Access Control Model

Chen Zhao, Nuermaimaiti.Heilili, Shengping Liu and Zuoquan Lin
Department of Information Science, Peking University
Beijing 100871, China
{zchen,nur,lsp,lz}@is.pku.edu.cn

Role-Based Access Control (RBAC) has been recognized as a strategy which reduces the cost and complexity of security administration in large-scale networked applications. A general family of RBAC models called RBAC96 was proposed by Sandhu *et al.* [1], which formally defines the relations among user, role and permission using the notion of set membership. Constraints is an important aspect of RBAC, which impose restrictions on acceptable configurations of the different components of RBAC. Nevertheless, it was discussed informally in the RBAC96 model.

There has been some efforts to present a logical framework for the access control models. Most of these works are based on first-order logic or its extensions. However, excessively rich expressiveness may bring on complex computation and confusion.

We present a novel formalization of RBAC using a description logic approach. Compared with first-order logic, DLs achieve a better tradeoff between the computational complexity of reasoning and the expressiveness of the language. We choose the DL language $\mathcal{ALC}$ to represent core and hierarchical RBAC, and $\mathcal{ALCQ}$ that extends $\mathcal{ALC}$ by *qualified number restrictions* to express RBAC constraints, including *separation of duty* and *role cardinality*. Based on our logical framework it is feasible to reason about RBAC and check the consistency of RBAC with constraints via a DL reasoner(e.g. RACER).

References

[1] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman. Role-based access control models. *IEEE Computer*, 29(2):38–47, 1996.