A UML PROFILE FOR ROLE-BASED ACCESS CONTROL

SUMMARY

When building an access control aware system, domain specifications are designed typically separate from security specifications. Main reason of this separation is representing security design models as structured text like policy files on the other hand visualizing domain specifications by graphical models like Unified Modeling Language (UML) models. This causes a gap between security modeling and system design modeling. Even if security modeling is structured at the early phases of development, security mechanisms are placed in to the system at the final phases, this causes another gap in the middle. These gaps affect security and maintainability of the resulting system in a bad way.

This study presents a solution that uses Model Driven Architecture (MDA) approach for bridging these gaps. A UML Profile for Role-Based Access Control (RBAC) is proposed. With this UML Profile, access control specifications can be modeled graphically together with problem domain specifications from the beginning of the design phase, making it possible to extend security integration over the entire development process.

Major contribution of this study is introducing a UML Profile for RBAC, to integrate security specifications of access control into the development process from the beginning; to form a well-defined Platform Independent Model (PIM) that can be used to automatically generate the corresponding Platform Specific Model (PSM) or generate code directly by transformation functions; to maintain technology independence and reusability, transformation functions handle technology-specific details; to simplify the work of developers; to benefit from the advantage of wide-range of commercial and non-commercial Computer-Aided Software Engineering (CASE) tools support by using easily interchangeable and lightweight UML extension mechanism. Additional contributions are employing significant RBAC constraints like Static Separation of Duty (SSD) and Dynamic Separation of Duty (DSD) into the profile, and introducing how Object Constraint Language (OCL) is used to validate well-formedness (syntax) and meaning (semantics) of information models against the RBAC.