Formal specification of access control Model for relational databases using UML and OCL

Ebaa Saoud

Systems Software Department, Odessa National Polytechnic University, UKRAINE, Odessa, 1, Shevchenko avenue,
E-mail: bblack@inbox.ru

In the corporate information systems (CIS) users data access control (AC) is mostly formalized by models *DAC*, *RBAC* and *MAC*. To reduce the complexity of the setup process of AC DBMS, it is important to automatize some of its stages. Automatization can be effectively performed when using MDA- methodology of software code development (Model Driven Architecture), which requires formal specification of the subject area description. Most products use *UML* language to represent meta-model that describes the behavior of AC models, using class diagram and interaction, and also use language O*CL (Object Constraint Language)* as the language of the constraints and the existing objects description. Most meta-models do not take into account the database properties, developed for an organization, its employees may be classified after structural and position hierarchy of subordination, and the database may already have data about this hierarchy.

In this paper, the modification of the meta-model of formal UML specification is proposed, which takes into account the specified feature. The model includes classes: *User* - users, *DBrelation* - DB model, *Role* - roles hierarchy of RBAC- model, *SecurityLevel* - hierarchy of security labels of MAC-model, *Permition* – access permissions at the SQL-level, *Category* - abstract class for combining of different models of AC, *Constraint* - *OCL*-constraints for the installation of access rights with taking into consideration of the structural and position hierarchy of users subordination, presented in the CIS database.

To validate the structures of the proposed model formalization of AC, editor Argo / UML is used, but for verification OCL-constraints the package *Dresden OCL* is used.

The proposed formal specification will allow to automate the choice of user roles classifier, taking into account AC model, the choice of user roles, taking into account a classifier, the choice of access objects classifier, represented in a relational database model CIS, the choice of the roles access right to the access objects and rules for access rights furnishing that exist in the DBMS.

*Переклад виконано Малиновською О. А., центр іноземних мов «Universal Talk», **www.utalk.com.ua***

Формальна специфікація моделі управлення доступом в реляційних базах даних з використанням мови UML та OCL

Ібаа Сауд

Кафедра системного програмного забезпечення, Одеський національний політехнічний університет,
УКРАЇНА, м.Одеса, проспект Шевченка, 1,
E-mail: bblack@inbox.ru

Робота присвячена першому етапу автоматизації процесу налаштування механізмів управління доступом на рівні СУБД - формалізації вимог з управління доступом з використанням мови графічних специфікацій UML і мови текстових специфікацій OCL.

Ключові слова – база даних, управління доступом, *RBAC, UML, OCL, Model Checking, MDA, MDS.*

I. Вступ

В корпоративних інформаційних системах (КІС) управління доступом до даних (УД) користувачів формалізується основними трьома моделями [1]: виборча (*DAC*), рольова (*RBAC*) і повноважна (*MAC*). В різних предметних областях використання цих моделей зростаюча кількість суб'єктів і об'єктів доступу призводить до високої трудомісткості процесу налаштування механізмів УД. Особливо це проявляється на рівні СУБД, як безпосередньо пов'язаному з управлінням даними. Природним шляхом вирішення цієї проблеми є автоматизація процесу налаштування механізмів УД на рівні СУБД як процесу проектування програмного коду збережених процедур і тригерів. В роботі [2] при автоматизації програмного коду механізмів УД різних СУБД передбачається наявність КІС в організації, співробітників якої можна класифікувати за структурно-посадовою ієрархією підпорядкування, а в БД вже присутні дані про цю ієрархії. Але проведені експерименти з БД університету показали, що опис вимог без формальної специфікації призводить до появи конфліктів між повноваженнями в посадових інструкціях співробітників і правами доступу ролей співробітників-користувачів. Дана робота присвячена вирішенню цієї проблеми на основі формальної специфікації УД в БД.

II. Формальні специфікації в моделях управлення доступом

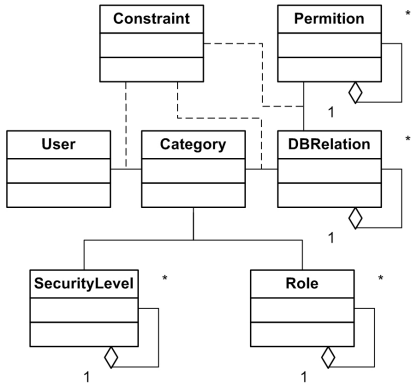
Сьогодні активно розвивається методологія розробки програмного коду під назвою *MDA* (*Model Driven Architecture*), частиною якої є *MDS*-методологія (*Model Driven Security*), які автоматизують процес розробки на основі формальних моделей. В них основною формальною мовою специфікацій є *UML* – мова моделювання у вигляді діаграм. В роботі [3] запропоновано розширення *UML* за назвою *ModelSec*,

яке формалізує специфікації для різних моделей УД, а в роботі [4] запропоновано уніфіковану мову моделювання управління доступом на основі *UML*. У зазначених роботах *UML* представляє мета-модель для опису поведінки моделей УД з використанням діаграми класів і взаємодії. Роботи [5-6] використовують мову *OCL* (*Object Constraint Language*) - мову опису обмежень на існуючі об'єкти.

Використання *UML* і *OCL* в процесі налагодження УД ефективно на етапі визначення вимог предметної області, коли необхідна виразність графічного подання *UML* з напів-алгоритмічністю *OCL*. Надалі для верифікації створюваних моделей УД необхідно вже використовувати логічні формалізації процесу *Model Checking*: дискрипційна логіка, завдання задоволення обмежень і логіка предикатів, які разом вимагають трансформації *UML* і *OCL* [5].

III. *UML-OCL* для управлення доступом в реляційних БД

Модифікацію мета-моделей формальних *UML*-специфікацій робіт [3-4], яка описує поведінку моделей *RBAC*, *MAC* та враховує існування в БД структурно-посадової ієрархії підпорядкування користувачів, представлено на рисунку.



Мета-модель формальної специфікації УД

Модель включає класи: *User* – користувачі, *DBrelation* - модель БД, *Role* – ієрархія ролей *RBAC*-моделі, *SecurityLevel* – ієрархія міток безпеки *MAC*-моделі, *Permition* – права доступу на рівні *SQL*-команд, *Category* – абстрактний клас для поєднання різних моделей УД, *Constraint* – організаційна ієрархія (атрибут *org_h*) та посадова ієрархія (атрибут *org_p*) для ролей. Атрибути *org_h*, *org_p* включають множину атрибутів з *DBrelation* та обмеження їх значень, які визначають ролі з *Role*.

Для валідації конструкцій запропонованої формальної моделі УД використано редактор *Argo/ UML* (*http://www.ArgoUML.com*), а для верифікації *OCL*-обмежень використано пакет *Dresden OCL* (*http://www.dresden-ocl.org*), який включає модулі: *OCLEditor* – редактор, *OCLParser*, *OCLTypeChecker* – синтаксичний і семантичний аналізатори, *OCLInterpreter* – динамічний валідатор відповідності *OCL* класів *UML*. Додатковий Модуль *OCL2SQL* може генерувати *SQL*-код з *check*-обмеженнями і тригерами [6].

Висновок

Запропонована *UML-OCL* формалізація моделі управління доступом в реляційній БД забезпечує суворий опис специфікації вимог, що зменшує невідповідність між вимогами посадових інструкцій співробітників по роботі з документами класу «для службового використання» і правами доступу співробітників-користувачів КІС до даних електронних документів в БД. Формальна специфікація дозволить автоматизувати вибір класифікатора ролей користувачів з урахуванням моделі УД, вибір ролей користувачів з урахуванням класифікатора, вибір класифікатора об'єктів доступу, представлених у вигляді реляційної моделі БД КІС, вибір права доступу ролей до об'єктів доступу і правил надання прав доступу, що існують в СУБД.

Література

[1] Тарасов, Д.О. Формальні моделі систем захисту інформації реляційних баз даних. / Д.О. Тарасов // Інформаційні системи та мережі. Вісник НУ "Львівська політехніка". – 2003. – № 489. – С. 296-306.

[2] Blazhko, A.A. Automated Design Method of Hierarchical Access Control In Database. / A.A. Blazhko, S.G. Antoshchuk, E. Saoud // Procs. of 5th IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. – Rende, Italy, 2009. – pp. 361-363

[3] ModelSec: A Generative Architecture for Model-Driven Security. / O. Sanchez, F. Molina, J. Garcıa-Molina, A. Toval // Journal of Universal Computer Science. – 2009. – № 15. – pp. 2957-2980

[4] Slimani, N. UACML: Unified Access Control Modeling Language. / N. Slimani., H. Khambhammettu , K. Adi, L. Logrippo // Procs. of 4th International Conference "New Technologies, Mobility and Security". – Quebec, Canada, 2011. – pp. 1-8.

[5] Brucker, A.D. A Model Transformation Semantics and Analysis Methodology for SecureUML / A.D. Brucker, J. Doser, B. Wolff // in Procs. of MoDELS. – Genoa, Italy, 2006. – pp. 306-320.

[6] Demuth, B. OCL as a Specification Language for Business Rules in Database Applications. / B. Demuth, H. Hussmann, S. Loecher // Procs. of 4th international conference on the Unified Modeling Language (UML 2001). – Toronto, Canada, 2001. – pp.104-117.