УНІФІКАЦІЯ СТРУКТУР УПРАВЛІННЯ ДОСТУПОМ ДО ДАНИХ ЗАСОБАМИ СУБД

Сауд Ибаа

Науковий керівник - доц. каф.«Системи програмного забезпечення»

канд. техн. наук О.А. Блажко

У корпоративних інформаційних системах (КІС) механізми управління доступом до даних реалізуються з використанням виборчої (*DAC*) і повноважною (*MAC*) політик безпеки. Необхідність деталізації опису об'єкта безпеки до рівня кортежу у вигляді *RLS* (*Row Level Security*) [1] вимагає створення додаткових механізмів зусиллями розробників СУБД з використанням свого способу реалізації політики безпеки, що ускладнює процес її включення в роботу КІС. Метою даної роботи є уніфікація структур з управління доступом до даних, які пропонуються різними СУБД, для зменшення трудомісткості адміністрування.

У роботі запропоновано уніфікувати алгоритм управління за рахунок шаблонів управління у вигляді четвірки *<dbms, policy, alg_type, pattern>*, де *dbms* - тип СУБД (*Oracle, IBM DB2, MS SQL, Sybase, PostgreSQL, UNI*); *policy* Є {*MAC*, *DAC*} - тип політики управління доступом; *alg_type* Є {*Native, Schema*} - алгоритм реалізації політики, який використовує вбудовані команди з управління доступом (*Native*) або заснований на користувацьких схемах даних (*Schema*); *pattern* - шаблон команд по управлінню доступом. Шаблони команд включають змінні: *#user_name#* - ім'я користувача, *#table_name#* - ім'я таблиці, *#column_name#* - ім'я атрибута таблиці, який бере участь в обмеженні доступу користувача до картежів таблиці (для *DAC*) або зберігає мітки конфіденційності (для *MAC*), *#label_list#* - список значень рівнів і міток доступу, *#user_view#* - предикат умов обмежень доступу до картежів таблиці. Уніфікація процесу управління доступом передбачає скорочення різниці в описі команд для різних СУБД.

Алгоритм автоматизації повинен отримувати вміст шаблонів, що зберігаються в зовнішньому джерелі і заміняти позначення змінних на пропоновані значення в ході установки системи управління доступом в залежності від значень *dbms, policy, alg_type*.

Подальший розвиток механізмів управління доступом передбачає створення методу вибору політики (*DAC, MAC*), алгоритму управління (*Native, Schema*) з урахуванням предметної області функціонування БД і типу СУБД за критеріями мінімального часу виконання запиту і мінімальної трудомісткості процесу адміністрування.

Список літератури:

1. Row-level Security in A Relational Database Management System / / Patent N 7240046 B2. - 2007. - United States Patent.