УДК 004.056

Микитюк І.С.
Войтович О.П.

ЗАХИСТ БАЗ ДАНИХ, ШЛЯХОМ ФРАГМЕНТУВАННЯ КОРИСТУВАЦЬКОГО ДОСТУПУ

Вінницький національний технічний університет

Анотація

В даній роботі проводиться аналіз захисту сучасних систем керування базами даних. На основі аналізу існуючих засобів захисту було виділено одну з проблем, рішення якої було запропоновано та реалізовано у вигляді моделі системи з модульною архітектурою і багатошаровим захистом від несанкціонованого доступу. Було представлено приклад реалізації загрози, та комплексне рішення у вигляді підходу до надання прав користувачам шляхом фрагментування доступу, що дозволить їй запобігти.

Ключові слова: база даних, захист баз даних, багатошаровий захист, шифрування, гешування.

Abstract

This research work describes analysis of protection of modern database management systems. One of the problems was presented on the basis of an analysis of existing remedies. The solution was proposed and implemented as a system with modular architecture and multilayer protection against unauthorized access. An example of the threat implementation was presented. The research work allows you to get a comprehensive solution to this problem in the form of an approach to granting rights to users by fragmenting user access.

Keywords: database, database protection, multilayer protection, cryptographic algorithms, hash.

Вступ

У ході збільшення та поширення інформації, якою може володіти людина у неї з'явилась необхідність обробки, структуризації та зберігання інформації. Відповідно до області використання даної інформації вона набуває великої цінності і втрата чи несанкціонований доступ до неї можуть нести важкі матеріальні наслідки для власника.

У ході пошуку оптимальної моделі бази даних, яка зможе повноцінно функціонувати та захищати користувацькі дані було прийнято рішення, яке свідчить, що електронні варіанти баз даних [1] є найзручнішим та найоптимальнішим вибором. З розвитком інформаційних систем та персональних комп'ютерів в цілому бази даних почали удосконалюватись і на сьогоднішній день пропонують зручне маніпулювання інформацією у базах, можливість рольового розмежування доступу до інформації у базі даних [2], та спрощення інтерфейсу для зручності у використанні та освоєнні інтерфейсу.

Проте серед сучасних засобів керування базами даних важко зустріти програмний засіб, який може запропонувати користувачеві максимально можливу захищеність інформації від зловмисника. Вони мають низку криптографічних методів, які можуть шифрувати та гешувати інформацію, в додаток до цього вони мають низку прав, які відповідають за регулювання доступу до інформації, а також налаштування, стосовно рольового доступу, проте вони мають проблему, яка зв'язана з отриманням авторизованим користувачем відповідних йому прав, а саме ті випадки, коли зловмисник отримав необхідну йому автентифікаційну інформацію [3]. Мова йде про програмний засіб, який запропонує компаніям, не тільки функції, які є у більшості СКБД, а і покращення наявних засобів та перетворення усіх їх у кращий комплексний підхід.

Метою даної роботи є аналіз проблем захисту у сучасних СКБД, та побудова власного багатошарового захисту, який дозволяє вирішити дані проблеми.

Для досягнення мети необхідно розв'язати такі задачі:

- проаналізувати проблеми у захисті сучасних СКБД;
- розробити багатошарову систему для вирішення проблем захисту інформації у СКБД.

Аналіз проблеми захищеності сучасних СКБД

Сучасні СКБД можна характеризувати як програмні засоби з високим ступенем захищеності інформації, яка зберігається в базах даних під їх управлінням, проте у ході аналізу баз даних було виявлено один з недоліків [4], а саме використання одного бар'єру для підтвердження користувачем

наданих йому привілеїв.

При представленні проблеми було виділено таку ситуацію при використанні будь-якої з популярних на сьогодні СКБД користувачі мають певні ролі, які надають їм привілеї [5], зображені у таблиці 1.

Роль	Можливості	Загрози
Власник	Усі дії по налаштуванню та обслуговуванню БД та видалення	Втрата даних у зв'язку з некомпетентністю чи халатністю,
Адміністратор	Адміністрування бази даних, надання привілеїв.	Цілісність даних, ненавмисне надання прав іншим користувачам.
Редактор	Редагування та видалення даних у таблицях	Цілісність та конфіденційність даних
Читач	Зчитування даних	Конфіденційність даних
Користувач без прав на доступ	Не може виконувати дії з БД	-

Таблиця 1 – Ролі користувачів у сучасних СКБД

Проаналізувавши загрози було виявлено ті, що можуть бути реалізовані відповідними користувачами можна зробити висновок, що кожен користувач має права, які він підтверджує. Сучасні бази даних надають права по користуванню базою даних після автентифікації користувача з необхідним рівнем доступу, тобто зловмиснику стає доступним рівень доступу користувача, в якого він міг отримати автентифікаційні дані, що на сьогодні не є найкращим рішенням у зв'язку з великою низкою каналів витоку та несанкціонованого отримання користувацьких даних.

Для роботи з базою даних з точки зору безпеки в реальних умовах створюється достатня кількість проблем, які зв'язані з користувацькою авторизацією. Це можуть бути, як проблеми звичайного підглядання паролю, так і проблеми крадіжок необхідних даних шляхом використання власних користувацьких автентифікаційних даних з невідповідною високою користувацькою роллю.

З цього можна зробити вихід, що сучасні СКБД, які мають слабкий парольний захист, чи потребують більшого рівня захисту потребують покращення автентифікаційної системи, яка буде мати на меті розбиття рівнів доступу користувачів і рівнів автентицікації.

Для аналізу та висування пропозицій слід перелічити деякі з реалізацій загроз, наведених у табл. 1.

Загроза отримання зловмисником автентифікаційних даних відповідної ролі:

1) Читач бази даних дасть змогу зловмиснику вкрасти інформацію.
2) Редактор дасть змогу відредагувати інформацію у БД.
3) Адміністратор дасть змогу приховано надати права користувачам, що не мають відповідного рангу.
4) Власник ставить під загрозу існування бази даних вцілому.

Проаналізувавши загрози можна зробити висновок, що однорівневий захист є проблемою, яку необхідно вирішити, і яку вирішує дана модель захисту інформації у базах даних.

Побудова багатошарової системи захисту інформації

Для забезпечення належного захисту інформації слід комбінувати найкращі існуючі напрацювання, але фрагментувати їх використання на «рівні захисту». Це дасть деякі переваги: користувач, який не володіє необхідним набором автентифікаційних даних отримає доступ тільки до відповідного рівня взаємодії з базою даних.

Першим і початковим рівнем є автентифікація користувача, яка дозволяє зловмиснику отримати *перший рівень доступу* до інформації у БД, прикладом якого може бути реалізація агротиму авторизації за допомогою введення комбінації логіну та паролю.

Отримавши перший рівень користувач, який хоче відредагувати інформацію має підтвердити свої права редактора для отримання доступу до функцій, які знаходяться на *другому рівні доступу*.

Прикладом реалізації підтвердження прав на отримання прав другого рівня може бути сутністю, яка використовує алгоритми гешування і зберігає геш-значення з таблицею, до якої хоче отримати доступ, поки що, звичайний користувач. Для переходу на другий рівень користувачеві пропонується ввести

графічний пароль, та вибрати геш-функцію, яка повинна до нього примінитись. Після введення даних вони зіставляються з даними, які прив'язані до БД і після правильного введення надає доступ.

Третій рівень доступу представляє з себе підтвердження доступу користувачем, наприклад шляхом наявності флешки-ключа. При запиті на отримання найвищих прав користувачеві виводиться повідомлення, яке пропонує йому вставити флешку з файлом, який містить необхідне для підтвердження прав геш-значення, яке було випадково згенероване під час створення самої БД і відвантажене на флешку. При наявності необхідного файлу його дані скануються та зіставляються з наявними даними у БД.

Відповідно до наведених прикладів необхідний багаторівневий захист може бути гнучко реалізований, і може надавати адміністратору БД можливість визначити необхідні шари захисту для конкретної таблиці чи БД.

Реалізувавши ці три рівні перед зловмисником, який хоче видалити БД, зламавши пароль зупиниться на шарі захисту, який пропонує вибір геш-функції та введення графічного паролю, до якого вона буде застосовуватись, після цього йде наступний шар – наявність флешки з файлом-ключем, і наприкінці дана модель буде слідкувати та співставляти отримані автентифікаційні дані з списком ролей та відповідним йому списком користувачів і не дасть доступ зловмиснику, який отримав автентифікаційні дані одного користувача, графічний пароль та геш-функцію другого користувача, а флешку в третього користувача.

Висновки

Виконаний аналіз сучасних СКБД показав один з недоліків вбудованих в них засобів захисту в плані надання доступу до функцій по адмініструванню базами даних групам користувачів. Саме тому пропонується підхід, який передбачає включення багатошарового захисту інформації шляхом використання засобів криптографії, графічного паролю, що збільшить час, потрачений на процес отримання необхідних користувачеві привілеїв, але дозволить відслідковувати та керувати доступом користувачів і захищати перш за все цілісність даних краще, чим це було реалізовано до цього.

Подальші дослідження будуть направлені на реалізацію та розвиток запропонованого підходу та дослідження показників продуктивності, безпеки та зручності використання даної моделі, залежно від конкретних реалізацій шарів захисту інформації.

REFERENCES

1. Зрюмов, Е. А. Базы данных для инженеров: навчальний посібник / Е. А. Зрюмов, А. Г. Зрюмова; Алт. держ. техн. ун-т им. И. И. Ползунова. – Барнаул : Видав-во АлтГТУ, 2010. – 131 с.
2. Шайтанова Н. Ж., Туленгалиева М.Г. Защита информации в базах данных [Електронний ресурс]. Режим доступу: URL : http://www.rusnauka.co m/10_DN_2014/Informatica/3_165120.doc.htm – Назва з екрану.
3. Полтавцева М. А., Хабаров А. Р. Безопасность баз данных: проблемы и перспективы //Программные продукты и системы. – 2016. – №. 3 (115).
4. Микитюк І.С., Баришев Ю.В. Підхід до захисту баз даних: тези на наукову конференцію, Вінницький національний технічний університет – 2017р.г
5. Microsoft Docs. Роли уровня баз даных. [Електронний ресурс]. Режим доступу: URL: https://docs.microsoft.com/ru-ru/sql/relational-databases/security/authentication-access/database-level-roles - Назва з екрану.
6. Захист програмного забезпечення. Частина 2 : навчальний посібник / В. А. Каплун, О. В. Дмитришин, Ю. В. Баришев – Вінниця : ВНТУ, 2014. – 105 с.

Іван Сергійович Микитюк – студент групи БС-14б, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: mikityukchanel@gmail.com

Олеся Петрівна Войтович – доц. кафедри захисту інформації, Вінницький національний технічний університет, email: voytovych.op@gmail.com

Ivan S. Mikitiuk – student, Faculty of Information Technology and Computer Engineering, Vinnytsa National Technical University, Khmelnytske shosse 95, Vinnytsia, email: mikityukchanel@gmail.com

Olesia P. Voitovych — Assistant Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, email: voytovych.op@gmail.com