УДК 004.056

Микитюк І.С
Баришев Ю.В.

ПІДХІД ДО ЗАХИСТУ БАЗ ДАНИХ

Вінницький національний технічний університет

Анотація

В даній роботі описуються різні способи захисту баз даних у сучасних СКБД, деякі методи захисту інформації та їх використання для захисту баз даних у подальшому. На основі аналізу існуючих способів засобів баз даних були визначені шляхи їх удосконалення, які були реалізовані у вигляді підходів до створення захищеної системи керування базами даних.

Ключові слова: база даних, захист даних, система керування базами даних, шифрування, гешування.

Abstract

This research work describes the various ways to protect data in modern database management systems, some methods of protecting information and their usage for data protection in the future. Ways of improvements databases was identified by using analyze of existing databases protect ways. Ways realized in approaches to creating a secure database management system.

Keywords: database, data protection, database management system, cryptographic algorithms, hash.

Вступ

Сучасна людина володіє різноманітною інформацією. Це як данні про акторів у фільмах та учасників улюблених музичних гуртів, так і інформація про будь-які події, які відбуваються на виробництві. Відповідно до цього сучасна людина прийшла до структурування цієї інформації шляхом створення баз даних.

Оскільки дана інформація може мати властивість прив’язувати до себе деякі матеріальні цінності відповідно з розвитком баз даних з’явились люди, які посягають на конфіденційність інформації, яка зберігається.

Зрозумівши, що електронні варіанти баз даних [1] зручніші за паперові бази даних люди почали удосконалювати їх роботу і на сьогодні будь-якому користувачеві чи управлінцю пропонують низку найрізноманітніших систем керування базами даних.

Сучасні системи керування базами даних розраховані для широкого користувачів користувача, а тому пропонують зручне керування, можливість рольового розмежування доступу до інформації у базі даних, та спрощення інтерфейсу для зрозумілості навіть найвіддаленішому від інформаційної сфери користувачеві.

Але склалось так, що у цій сфері серед великої кількості подібних СКБД досить рідко зустрічається програмний засіб, який може похвалитись своєю захищеністю від зловмисника. Такий програмний засіб, який запропонує компаніям, які досить високо оцінюють свою внутрішню інформацію належний її захист, та дасть керівникам повний інструментарій заходів, які захистять внутрішню інформацію компанії, як шифруванням інформації, так й її гешуванням.

Метою даної роботи є удосконалення захисту конфіденційності інформації, яка зберігається у базах даних.

Для досягнення мети необхідно розв’язати такі задачі:

- проаналізувати сучасні СКБД;
- розробити підхід до комплексного захисту баз даних;
- розробити захищену СКБД на основі цього підходу.

У даній роботі представлені результати розв’язання перших двох задач.

Аналіз сучасних систем керування базами даних

На сьогодні кожна СКБД пропонує своєму користувачеві досить поширений на сьогодні рольовий доступ до даних у БД, деякі з них забезпечують високий рівень захисту цілісності інформації.

MySQL – одна з найпопулярніших СКБД з відкритим кодом сьогодення, яка пропонується користувачеві для створення динамічних веб-сторінок, є складовою багатьох популярних серверів. Але з точки зору захисту у цієї СКБД є низка недоліків. Перший з них – це недостатньо суворий набір вимог щодо паролів користувачів. На сьогодні MySQL не має належного захисту від прямого

перебору паролів, вона не примушує користувача створити належний пароль для свого облікового запису. Ця СКБД пропонує користувачеві створити належні привілеї для кожного користувача чи групи користувачів і за належного адміністрування може бути вельми захищеною, але на сьогодні цього недостатньо для того, щоб сказати, що ця СКБД є гарним вибором для інформації, втрата якої спричинить суттєві збитки.

Oracle – СКБД, розробники якої змогли попіклуватись про те, щоб інформація, яка буде зберігатись у базах даних, створених саме їхньою СКБД буде вважатись «краще захищеною, ніж у конкурентів», тому там вже можна побачити таке доповнення, як Oracle Advanced Security, яке дозволяє шифрувати увесь потік даних. Network encryption теж допоможе користувачеві захистити його дані у мережі. Розробники пропонують користувачеві такі алгоритми, як AES, DES, Triple-DES [2]. Також тут є аудит доступу до даних та жорсткіші вимоги до захисту облікових записів користувачів (захист від перебору паролю, вимоги до створення паролю облікового запису та інше). Але для того, щоб даний захист запрацював у пересічного користувача йому потрібен кваліфікований адміністратор СКБД, який зможе відлагодити рівень захисту інформації на належному рівні та знає про ці всі засоби захисту. Тому слід зауважити, що на сьогодні вся потужність усіх засобів захисту у даній СКБД не використовується на сьогодні через те, що потенційним користувачам простіше заплатити за розробку власної СКБД через те, що більшість замовників не хочуть сподіватись на підтримку потрібних їм функцій захисту від розробника СКБД, яку вони купують. Так, як стартовий захист у СКБД є звичайним парольним разом з гарними засобами захисту Oracle не може запропонувати користувачеві гарантію захищеності даних без належного налаштування їхньої СКБД.

MS Access – доволі популярна на сьогодні і проста СКБД, яка дозволяє користувачеві на інтуїтивному рівні створити свою базу даних, і захистити її на основі створення паролю чи навіть робочої групи. Має низку налаштувань безпеки, які сильно програють конкурентам.

Проаналізувавши сьогоднішній стан безпеки систем керування базами даних можна виділити тенденцію розробників з точки зору захисту: кожна СКБД має розмежування доступу до інформації в базах даних за допомогою створення користувачів, ролей, захисту цілісності шляхом створення резервних копій та інших функцій, які можуть бути доступні тільки користувачеві, який має освіченого адміністратора, но жодна з сучасних СКБД не може запропонувати захищеність інформації користувача відразу ж після створення.

Підходи до створення захищених СКБД

Для того, щоб створити СКБД, яка буде для інформації «фортецею» слід зрозуміти, що вона повинна не лише мати приємний інтерфейс, рольовий доступ, вимагати від користувача належного захисту власного облікового запису і додатково з самого створення бази даних мати на меті зашифрувати інформацію та захистити саму СКБД від зловмисників.

У загальному про покращення захисту слід сказати те, що спочатку інформація у тільки створеній СКБД повинна шифруватись. Для цього слід використати стандарт сьогодення, а саме AES [3]. Відповідно до цього інформація не буде доступною зловмиснику, який обійшов можливу парольну автентифікацію. Також слід використати гешування паролю доступу користувача до бази даних, шифрування самої інформації у базі даних, так і використання ролей доступу до бази даних.Стадія гешування має за мету те, що геш-значення має бути унікальним для унікального набору даних, тому немає необхідності зберігати пароль у чистому вигляді – достатньо його геш-значення.

Підхід передбачає виконання таких етапів:

1) При першій авторизації для створення нового облікового запису користувач записує свої дані у СКБД;

2) СКБД записує дані користувача, але пароль користувача записує в загешованому вигляді, тому при несанкціонованому доступу зловмисник не зможе получити готовий пароль для підключення до захищених відділів СКБД;

3) При авторизації у базі даних користувач вводить свої дані, а СКБД шукає запис з ім’ям і геш-значенням паролю, з яким буде співставлятись загешований введений при авторизації пароль користувача і при правильному проходженні цього процесу дасть доступ користувачеві до інформації, яка доступна для наданих привілеїв користувача.

Також для посилення захисту самої бази даних відповідну геш-функцію можна використати для гешування атрибутів таблиць чи навіть назв таблиць, які можуть прикріплюватись як до конкретних даних користувача, так і до інших даних, які вимагатиме програма. Пошук даних повинен виконуватись по закритій базі, також для неможливості зламу СКБД ззовні повинен бути

реалізований захист від дампінгу [4] – доступу до дампів пам’яті, які містять важливу інформацію бази даних користувача.

Висновки

Виконаний аналіз сучасних СКБД показав недостатність вбудованих в них засобів захисту для пересічного користувача, що обумовлено складністю їх адміністрування та відсутністю комплексного підходу до розробки модулів захисту інформації цих СКБД. Саме тому пропонується підхід, який передбачає широке використання засобів криптографії для забезпечення захисту даних та засобів захисту програмного забезпечення для захисту самої СКБД, що зменшить продуктивність обробки даних, однак дозволить підвищити рівень захисту даних. Подальші дослідження будуть направлені на реалізацію запропонованого підходу та дослідження показників продуктивність/безпека залежно від конкретних реалізацій модулів захисту інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

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. Сучасні криптографічні системи: Навч. посібник. – Одеса: ВЦ ОНАЗ ім. О.С. Попова, 2007. – 152 стор.
3. Хабрхабр. Как устроен AES [Електронний ресурс]. Режим доступу: URL: https://habrahabr.ru/post/112733/ - Назва з екрану.
4. 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

Юрій Володимирович Баришев – к. т. н. кафедри захисту інформації, Вінницький національний технічний університет, email: yuriy.baryshev@gmail.com

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

Baryshev Yurii — Cand. Sc. (Eng), Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, yuriy.baryshev@gmail.com