УДК 621.398.96
Р. Ю. ЛИСИЙ,
Державний університет телекомунікацій, Київ

ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ УПРАВЛІННЯ БАЗАМИ ДАНИХ

Розглянуто сучасні технології та принципи, використовувані для захисту баз даних (БД) і систем управління базами даних (СУБД).

Ключові слова: захист даних; управління доступом; модель безпеки; автентифікація; шифрування; протоколювання і аудит; оператори SQL.

Вступ

При зберіганні та обробці даних у будь-якій СУБД одне з головних завдань користувача — подбати про безпеку цих даних.

Дані в системах баз даних мають зберігатися з додержанням конфіденційності та безпеки. Інформація не повинна бути загублена або викрадена. Під забезпеченням безпеки даних у базі розуміють захист даних від випадкового чи спланованого доступу до них осіб, які не мають на це права, а також від несанкціонованого розкриття, зміни або вилучення.

З огляду на важливість безпекових питань спинимося на результатах аналізу основних сервісів безпеки, а також якісного оцінювання механізмів захисту та моделей безпеки, аби визначити ефективні технології забезпечення захисту баз даних у сучасних СУБД.

Головною формою організації інформаційних масивів в інформаційних системах є бази даних, а найбільш поширеною моделлю даних у БД є реляційна модель [1]. Системи управління базами даних, особливо реляційні, стали незамінним інструментом зберігання великих масивів інформації.

Варто наголосити, що головні вимоги із забезпечення безпеки бази даних і СУБД багато в чому такі самі, як вимоги стосовно безпеки даних у комп'ютерних системах: контроль доступу, криптозахист, перевірка цілісності, протоколювання і т. ін.

Основна частина

Для організації управління доступом використовуються, зокрема, такі моделі безпеки: *дискреційна*, *мандатна* і *рольова*. Способом формалізованого подання ***дискреційного доступу*** є матриця доступу або списки управління доступом, що встановлюють перелік не лише користувачів, а й дозволених операцій стосовно кожного об'єкта БД. Підходи до побудови дискреційного управління доступом реалізуються за допомогою таких моделей, як децентралізована, централізована та мішана, причому саме мішаний варіант реалізовано в більшості СУБД.

Мандатна модель, яка поєднує в собі захист і обмеження прав у сфері комп'ютерних процесів, даних і системних пристроїв, має на меті запобігати їх небажаному застосуванню. Для СУБД мандатна модель безпеки може розширювати чи замінювати дискреційний контроль доступу та навіть концепцію користувачів і їх груп. Права доступу кожного суб'єкта, як і відповідні характеристики конфіденційності, знаходять відображення у вигляді сукупності, яка включає в себе рівень конфіденційності та набір категорій. Для реалізації вимог безпеки на базі мандатної моделі рядкам і стовпцям матриці БД приписують мітки, які далі надають користувачам. Вочевидь, ефективне застосування мандатної моделі можливе тільки разом із дискреційною.

Що ж до ***рольової моделі***, то вона працює в розвиток політики вибіркового управління доступом, коли права доступу суб'єктів системи до тих чи інших об'єктів групуються з урахуванням специфіки їх використання, визначаючи цим самим роль кожного суб'єкта системи. Управління правами доступу здійснюється або на основі матриці доступу, або за правилами, що регламентують поведінку (ролі) користувачів та їх активацію під час сеансів. Рольове розмежування доступу дозволяє реалізувати динамічні правила надання доступу. Гарантією безпеки в цій моделі виступає чітке визначення ролі як адміністратора БД, так і її користувача стосовно права доступу до об'єктів БД і прав на читання, модифікацію, запис і вилучення цих об'єктів. Технологія управління доступом на основі ролей настільки гнучка й потужна, що дає змогу змоделювати як вибіркове, так і мандатне управління доступом [2].

Для будь-якої захищеної БД процедури *ідентифікації*, *автентифікації* та *авторизації* є обов'язковими. Процедура ***ідентифікації*** полягає в призначенні користувачеві, який виступатиме споживачем ресурсів сервера БД, певного імені. Ім'я користувача являє собою унікальну мітку, що відповідає прийнятим угодам і забезпечує однозначну ідентифікацію об'єкта реального світу в просторі відображуваних об'єктів. Сутність

автентифікації полягає в підтвердженні автентичності користувача, що надав той чи інший ідентифікатор. ***Авторизація*** зводиться до визначення переліку конкретних інформаційних ресурсів, з якими автентифікованому користувачеві дозволено працювати. З погляду БД процедура автентифікації може бути як внутрішньою (засобами самої БД), так і зовнішньою, виконуваною засобами операційної системи (ОС) або мережі. У сучасних СУБД широко використовується зовнішня автентифікація на *біометричній основі*, автентифікація на базі володіння так званим *токеном*, а також *парольна* автентифікація, що ґрунтується на деякій специфічній словесній інформації.

Біометрична автентифікація — це процес доведення автентичності заявленого користувачем імені через надання ним свого біометричного образу. Біометричними характеристиками людини є відбитки пальців і долоні, звуки її голосу, вигляд обличчя, відбиток сітківки ока, особливості рухів і ходи, особливості роботи на клавіатурі, власний підпис. Результати системного аналізу з визначенням якісної оцінки сучасних біометричних датчиків відбитків пальця наведено в [3].

Серед заходів, що дають змогу значно підвищити надійність ***парольного захисту***, слід назвати такі: накладення технічних обмежень; управління терміном дії паролів, їх періодичну зміну; обмеження доступу до файла паролів; обмеження кількості невдалих спроб входу в систему; навчання і виховання користувачів; використання програмних генераторів паролів [4].

Цих заходів доцільно вживати завжди, навіть якщо поряд із паролями використовуються інші методи автентифікації, наприклад ті, які ґрунтуються на володінні ***токенами*** — предметами чи пристроями, здатними підтверджувати автентичність користувача. Розрізняють токени з пам'яттю (пасивні, які тільки зберігають, але не обробляють інформацію) та інтелектуальні (активні) токени. Найпоширенішим різновидом токенів із пам'яттю є картки з магнітною смугою. Їх використання потребує зчитувального пристрою, забезпеченого клавіатурою і процесором. Інтелектуальні токени характеризуються наявністю власної обчислювальної потужності. До них належать інтелектуальні картки, стандартизовані ISO, тощо.

Сьогодні одна з основних загроз для БД — це несанкціоноване копіювання даних або фізична крадіжка носія інформації. Найефективнішим методом боротьби з такими загрозами є ***шифрування даних***. За способом функціонування системи шифрування СУБД поділяють на два класи [5]: 1) системи прозорого шифрування, що підпорядковується адміністраторові; 2) системи непрозорого шифрування (викликаються користувачем).

У системах ***прозорого шифрування*** криптографічні перетворення здійснюються непомітно для користувача, оскільки його програми не зазнають змін. Системи прозорого шифрування можуть бути як вбудованими в СУБД, так і зовнішніми щодо цієї системи. При прозорому шифруванні використовується ключ шифрування БД, який зберігається в завантажувальному запису БД для доступності при її відновленні. Функція прозорого шифрування даних захищає «неактивні» дані, тобто файли даних і журналів. Системи ***непрозорого шифрування*** викликаються користувачем і можуть використовувати як засоби шифрування самої СУБД, так і зовнішні щодо СУБД утиліти.

Існують два основні види шифрування: ***симетричне*** і ***асиметричне***. У першому з них один і той самий ключ використовується і для шифрування, і для розшифрування повідомлень. У свою чергу, симетричне шифрування поділяється на потокове і блокове шифрування. Потоковий шифр можна перетворити на блоковий, розбиваючи вхідні дані на окремі блоки і шифруючи їх по одному. При цьому блокові шифри мають вищу криптостійкість, аніж потокові. Утім потокові шифри часто реалізуються в апаратному вигляді. Адже подання даних і їх обробка в потокових шифрах дуже близькі до відповідних процесів в апаратурі.

У разі асиметричного шифрування існують два ключі — несекретний і секретний. Перший використовується для шифрування і може публікуватися разом з адресою користувача, тоді як другий застосовується для розшифрування і відомий тільки одержувачу.

Асиметричні методи шифрування дозволяють реалізувати так званий електронний підпис, або електронне завірення повідомлення, ідею якого розкрито в [4]. Послуги асиметричного шифрування можна реалізувати і за допомогою симетричних методів, якщо є надійна третя сторона, що знає секретні ключі своїх клієнтів. Для компенсації недоліків симетричного шифрування широко застосовується комбінована криптографічна схема, в якій за допомогою асиметричного шифрування передається сеансовий ключ, що використовується сторонами для обміну даними за допомогою симетричного шифрування.

Криптографічні методи дозволяють надійно контролювати цілісність інформації. Криптографічна контрольна сума практично виключає всі можливості непомітної зміни даних. Сучасні СУБД включають у себе резервне копіювання і аудит як невід'ємні складові системи безпеки. Суть ***резервного копіювання*** полягає в зберіганні копії БД. При необхідності (несанкціоноване вилучення або модифікація БД) ця копія дає змогу відновити правильну версію БД.

Аудит полягає у відстежуванні всіх значущих з погляду безпеки подій, які зберігаються в текстовому файлі (Log-файл). Цей файл шифрується в разі застосування прозорого шифрування для підвищення захищеності БД від атак зловмисників.

Зауважимо, що аудит у поєднанні з протоколюванням має на меті забезпечення підзвітності користувачів і адміністраторів; уможливлення реконструкції послідовності подій; надання інформації для виявлення і аналізу будь-яких проблем [4]. Утім протоколювання істотно знижує продуктивність сервісів, надмірно обтяжуючи процес аудиту. Це зрештою навіть знижує інформаційну безпеку. Особливо важко досягти злагодженого протоколювання та аудиту в розподіленій різнорідній системі.

Насамкінець слід зазначити, що для захисту БД можна використовувати основні засоби мови **SQL**, такі як оператори надання і відміни прав доступу; збережені процедури і тригери; оператори для шифрування даних; резервне копіювання і відновлення даних. Тригер — це програмний блок, асоційований з таблицею БД, що автоматично виконує вказані в ньому дії, коли стосовно пов'язаної з ним таблиці відбулася певна подія. Збережена процедура — це модуль (іменований набір команд) мови SQL, що зберігається на сервері і є самостійним об'єктом БД.

Висновки

♦ У сучасних СУБД використовуються гібридні моделі забезпечення безпеки, до складу яких входять дискреційна, мандатна і рольова моделі.

♦ З-поміж усіх схем автентифікації найчастіше застовується парольний захист, що приваблює дешевизною і простотою.

♦ Набуває поширення автентифікація за допомогою токенів, а також біометрична.

♦ У СУБД домінує прозоре шифрування. Його перевага полягає в тому, що дані завжди зашифровано, хоча це створює додаткове навантаження на центральний процесор. Окрім того прозоре шифрування звільняє користувача від потреби змінювати свої програми.

♦ Спільне використання симетричних і асиметричних методів шифрування підвищує ефективність і зменшує завантаженість СУБД.

♦ Неодмінною складовою системи безпеки СУБД є системи резервного копіювання (відновлення) і аудиту. Резервне копіювання (відновлення) може здійснюватися через графічний інтерфейс, а також за допомогою команд SQL.

♦ Мова SQL відіграє важливу роль у захисті СУБД. За допомогою її команд можна реалізовувати практично всі аспекти захисту таких систем.

♦ Ефективний захист БД у СУБД можливий за умови комплексного, систематизованого підходу, із поєднанням різних сервісів і механізмів безпеки.

Список використаної літератури

*1. **Нечипоренко, О. В.** Классификационная схема моделей баз данных для лазерных технологических комплексов / О. В. Нечипоренко, С. А. Миценко // Вісн. ЧДТУ.— 2013.— № 2.— С. 48–54. — (Серія: технічні науки).*

*2. **Анализ** концептуальных подходов к обеспечению защиты баз данных [Електронний ресурс] // Мир компьютеров.— Режим доступу: http://compsmir.ru/?p=112*

*3. **Системний** аналіз біометричних датчиків відбитків пальця для системи управління доступом лазерного технологічного комплексу / [В. М. Лукашенко, Т. Ю. Уткіна, О. С. Вербицький та ін.] // Вісн. ЧДТУ.— 2012.— № 4.— С. 29–34.— (Серія: технічні науки).*

*4. **Галатенко, В.** Информационная безопасность [Електронний ресурс] / В. Галатенко // Открытые системы. СУБД.— 1996.— № 04.— Режим доступу: http://www.osp.ru/os/1996/04/178931/*

*5. **Шифрование** данных в СУБД [Електронний ресурс] // Мир компьютеров.— Режим доступу: http://compsmir.ru/?p=118*

*6. **Комаров, А.** Базу данных не стащить! Правильные способы защитить данные в таблицах БД [Електронний ресурс] / А. Комаров // Хакер.— № 04/09 (124).— Режим доступу: http://www.xakep.ru/magazine/xa/124/ 032/1.asp*

Рецензент: доктор техн. наук, професор **В. Л. Бурячок**, Державний університет телекомунікацій, Київ.

Р. Ю. Лысый

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Рассмотрены современные технологии и принципы, используемые для защиты баз данных (БД) систем управления базами данных (СУБД).

Ключевые слова: защита данных; управление доступом; модель безопасности; аутентификация; шифровка; протоколирование и аудит; операторы SQL.

R. Yu. Lysyi

DATEBASE MANAGEMENT SYSTEMS SECURITY TECHNOLOGIES

Modern technologies and principles using for database and database management protection are considered.

Keywords: date protection; access management; security model; authentification; ciphering; protocol puting and audit; SQL operators.