УДК 681.3.06: 519.248.681
Р. Козак
(Тернопільський національний технічний університет імені Івана Пулюя)

ЗАБЕЗПЕЧЕННЯ НАДІЙНОГО ШИФРУВАННЯ ДАНИХ В СУБД

Основна проблема при зберіганні важливої інформації в непідконтрольних СУБД пов'язана з можливістю витоку даних у процесі злому сервісу або в результаті неправомірних дій адміністраторів. Для рішення цієї проблеми в CryptDB забезпечена підтримка шифрування, при якій дані на стороні СУБД ніколи не фігурують у відкритому вигляді, а всі передані в СУБД запити містять тільки зашифровані дані, у тому числі в умовних блоках.

У проекті CryptDB зроблено спробу розв'язання проблеми безпечного зберігання даних у БД, що обслуговуються в хмарних сервісах і інших непідконтрольних системах.

При використанні CryptDB, у процесі виконання SQL-запитів всі дії виробляються тільки із зашифрованими даними, тобто користувач може відправити SQL-запит до СУБД і одержати результат без розшифрування інформації на стороні сервера (дані будуть розшифровані на обладнанні клієнта). Для забезпечення збереження конфіденційності інформації використовується багаторівнева система шифрування, при якій різні дані розміщаються на різних вкладених криптографічних рівнях, кожний з рівнів має свій ключ і підтримує обмежений набір найпростіших операцій над зашифрованими даними. Для приховання даних на кожному рівні використовуються свої методи гомоморфного шифрування, при яких дані не зворотно спотворюються, але зберігається можливість здійснення певних математичних операцій, які дадуть аналогічні результати, що й операції над вихідними даними (можна використовувати зашифровані дані для порівняння, сортування, додавання тощо без попереднього розшифрування, наприклад, виконується умова *decrypt(crypt(A) + crypt(B)) = A + B)*.

CryptDB реалізований у вигляді проксі, не потребуючої модифікації коду СУБД. Для виконання криптографічних операцій на стороні СУБД використовується набір додаткових функцій (UDF, user-defined functions).

Проксі складається із двох частин: спеціальної бібліотеки на мові C++ та модуля на мові Lua.

CryptDB підтримує зв'язування по ланцюжку ключів шифрування й паролів користувачів СУБД. При такій схемі роботи доступ до даних можуть одержати тільки користувачі, паролі яких прив'язані до ключів шифрування. Адміністратор СУБД, навіть одержавши якимось чином ключі шифрування, які фігурують на сервері, не зможе одержати доступ до даних, не знаючи паролів власників цих даних. Використання прив'язки ключів до паролів користувачів вимагає наявності в базі 11- 13 унікальних анотацій схем даних для захисту вмісту близько 20 полів, а також виправлення 2-7 рядків коду в web-додатку.

На відміну від інших подібних розробок, розробникам CryptDB вдалося забезпечити непогану продуктивність: у порівнянні зі звичайним MySQL використання CryptDB підвищує навантаження всього на 15- 26%. При роботі phpBB швидкість виконання операцій сповільнилася всього на 14,5%, при виконанні тестового набору TPC-C швидкість сповільнилося на 26%. Розмір збережених на диску даних при цьому виріс приблизно на 20%.