ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ЗА ДОПОМОГОЮ ЗАШИФРОВАНОЇ ОБРОБКИ ЗАПИТІВ

Ахтирцев І.І.
Науковий керівник – к.т.н., доцент Федюшин О.І.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Безпеки інформаційних технологій,
тел.702-14-25, e-mail: illia.akhtyrtsev@nure.ua, тел. (099) 797-20-40)

This work presents CryptDB, a system that explores an intermediate design point to provide confidentiality for applications that use database management systems (DBMSes). CryptDB leverages the typical structure of database-backed applications, consisting of a DBMS server and a separate application server In this work we discuss the threats that CryptDB defends against. Next, we describe prototype implemntation and evaluate the performance and security of CryptDB, as well as the effort required for application developers to use CryptDB, also we compared time of queries performance with using CryptDB and without. We made some conclusions.

Втрата приватної інформації є актуальною проблемою, у тому числі для інтернет-додатків. Зловмисник може використовувати спеціальне програмне забезпечення для отримання несанкціонованого доступу до серверів, адміністратори хостингу або постачальники програмного забезпечення можуть зловживати повноваженням та мати доступ до особистих даних або зловмисники з фізичним доступом до серверів можуть отримати доступ до всіх даних на диску та в пам'яті.

Нині існує велика кількість векторів атак та вразливостей в мережі, описанням яких займається спільнота OWASP. OWASP створив список з 10 найнебезпечніших векторів атак в мережі. Деякі з них несуть безпосередню загрозу для персональних даних користувачів на віддалених серверах.

Таким методом є SQL-ін’єкція, яка нараховує п’ять основних технік: оператор UNION, логічний метод, на основі помилок, метод з альтернативним каналом передачі даних, Time delay. Захист від атак такого типу вимагає фільтрації вхідних даних. І все це працюватиме, якщо адміністратори добросовісно робитимуть свою роботу. Та все ж існують ситуації, коли цього досягти неможливо.

Нині існує певна кількість робіт, які освітлюють цю проблему, у тому числі це роботи [1–3]. В них аналізуються загальні поняття гомоморфного шифрування, яке є основою для реалізації шифрованих запитів, а також наводиться опис принципів роботи додатку CryptDB, який є реалізацією даного механізму. Додаток CryptDB дозволяє приховувати персональні дані користувачів навіть від адміністраторів бази даних.

Метою даної роботи є виявлення ефективності гомоморфного шифрування для захисту особистих даних в інтернет-додатках за

критеріями швидкості виконання базових операцій і ступеню захищеності даних, тобто швидкості криптоаналізу. Також завданням роботи є пошук шляхів подальшого розвитку даного принципу для захисту особистих даних в інтернет-додатках.

В ході даної роботи була проведено налаштування додатку CryptDB. В якості тестового середовища була обрана операційна система Ubuntu 16.4., сервер бази даних MySQL 5.7, проксі CryptDB, а також клієнт бази даних. Ці додатки були встановлені в межах однієї системи. Для експерименту створена база даних, проводилося порівняння виконання запитів до MySQL бази даних безпосередньо, бази даних CryptDB та двох варіацій баз CryptDB proxy. Основними критеріями оцінки ефективності роботи CryptDB була швидкодія виконання запитів. Тобто в ході роботи ми порівнювали час виконання запитів. Результати заміру часу затримки виконання запитів до різних серверів, отримані в роботі [2], були підтверджені практично й мають наступний вигляд: час виконання запиту select до серверу MySQL з використанням CryptDB більший на 10%, delete – 14%, insert – 20%, update – 27%.

Таким чином, система CryptDB надає достатній рівень захищеності особистих даних, при цьому впливає на швидкодію виконання запитів не значною мірою. Це дає можливість забезпечувати конфіденційність даних в інтернет-додатках без відчутної для користувача втрати швидкодії. І найголовніше, система гомоморфного шифрування виключає будь-які погрози з боку адміністраторів бази даних.

Список джерел:

1. Poteya Manish M. Homomorphic Encryption for Security of Cloud Data / Poteya Manish M., Dhoteb, C. A., Sharmac Deepak H. //Procedia Computer Science 79, 2016,- P. 175–181. DOI: https://doi.org/10.1016/j.procs.2016.03.023.

2. Stupen, P. Application of homomorphic encryption for the protection of numerical data in cloud storage / Stupen P., V. Sokolov, S. O., Zolkina, O. Yu. //Scientific works of the Petro Mohyla Black Sea State University of the Kyiv-Mohyla Academy complex. Series: Computer Technology, Vol. 266, No. 254, P. 71–75, available at : http://nbuv.gov.ua/UJRN/Npchduct_2015_266_254_13 (last accessed: 28.11.2018).

3. R. A. Popa CryptDB: Apractical encrypted relational DBMS / R. A. Popa, N. Zeldovich, and H. Balakrishnan. //Technical Report MITCSAIL-TR-2011-005, MIT Computer Science and Artificial IntelligenceLaboratory, Cambridge, MA, January 2011.