УДК 004.056 : 004.424.47

О. М. Гайдаєнко

ЗАХИСТ SQL-БАЗИ ДАНИХ В ОПЕРАЦІЙНІЙ СИСТЕМІ ANDROID

Вінницький національний технічний університет

Анотація: *У статті запропоновано методи для захисту SQL бази даних в операційній системі Android. Методи ґрунтуються на використанні алгоритму TOTP(Time-based One Time Password Algorithm). Запропоновано алгоритм захисту бази даних за допомогою TOTP, а також спосіб блокування файлу бази даних через мережу Інтернет.*

Ключові слова: *захист бази даних, SQL, Android, TOTP.*

Abstract*: In this article presented methods to protect SQL database in operating system Android. Methods based on the use of the algorithm TOTP (Time-based One Time Password Algorithm). Offered an algorithm for database protection via TOTP, but also a way to lock the database file on the Internet.*

Keywords*: protection database, SQL, Android, TOTP.*

Захист персональних даних – одна найбільш актуальних тем сьогодення у сфері інформаційних технологій. Кожного для безліч користувачів зберігає персональні дані у мобільних додатках. Це може бути інформація про кредитні картки, облікові записи певних сервісів, а також автентифікаційні дані, які використовуються навіть на робочому місці особи. Тому, зберігаючи такого роду дані, потрібно бути обережним, оскільки велика кількість зловмисників постійно шукають спосіб отримання персональної інформації, яка у разі втрати може призвести не тільки до власних, а й до кооперативних матеріальних втрат.

На сьогоднішній день на 80% мобільних пристроїв використовується саме операційна система Android. Тому захист ресурсів саме цієї операційної системи є актуальним.

Метою дослідження є пошук оптимальних рішень для забезпечення захисту бази даних в операційній системі Android, а також спроба створити універсальних програмний засіб захисту, який можна буде легко інтегрувати у мобільний додаток.

Для вирішення даної проблеми запропоновано використання TOTP (Time-based One Time Password Algorithm) – достатньо стійкого до криптографічних атак алгоритму односторонньої автентифікації, який використовується для створення одноразових паролів на основі часу [1]. При цьому використовується не стале значення, а певний інтервал часу, який доволі важко взнати, якщо немає вихідних кодів програми. У програмному засобі пропонується реалізувати сервіс, який буде постійно працювати у фоновому режимі. Такий сервіс буде генерувати код на основі параметрів часу, який буде використовуватись як маска для генерування паролю доступу до бази даних. Тобто, коли програма працює, час від часу змінюється код доступу до бази даних і програмний засіб продовжує свою роботу. Використання цього методу є кращим, аніж використання автентифікації через СМС або за допомогою QR-коду, оскільки використання СМС-сервісу потребує коштів і вміст повідомлення може бути перехоплений. Що ж стосується QR-коду, то зазвичай користувачі не зовсім охоче сканують такого роду коди, а тим більше якщо кожного разу, заходячи у програму, необхідно відсканувати код для доступу до бази даних. У разі, якщо зловмисник отримає пароль доступу, він не зможе його використати, оскільки за умов використання паролю на основі часу пароль зловмисника буде не актуальним, застарілим. Тому можна вважати, що цей метод дозволить забезпечити доволі стійкий захист файлів бази даних.

Для того, щоб виконати шифрування бази даних буде використано SQLCipher – open-source розширення для SQLite, яке забезпечує шифрування файлів бази даних за допомогою алгоритму шифрування AES з використанням 256 бітного ключа [2]. AES – симетричний алгоритм блокового шифрування, який наразі використовується як стандарт шифрування [3]. Цей алгоритм є криптостійким, тому його використання є доцільним для забезпечення безпеки файлу бази даних.

Переваги цієї бібліотеки:

- відносно легке інтегрування у проект;

- використання стійкого алгоритму шифрування;
- наявність документації;
- схожість API з SQLite.

Існує твердження, що використання open-source бібліотек негативно впливає на захист додатку, так як зловмисник може проаналізувати вихідні коди і зламати захист. У нашому випадку використання такого роду засобів становить небезпеку, проте можна заплутати логіку, використавши при цьому пароль, який надходить у програму через сервіс, як маску, яка буде накладатись на ключ, який буде зберігатись у програмі. Враховуючи те, що пароль буде змінюватись часто, взнати пароль доступу до бази даних методом перебору буде дуже важко, а й навіть не можливо. На рисунку 1 наведено базову схему роботи додатку.

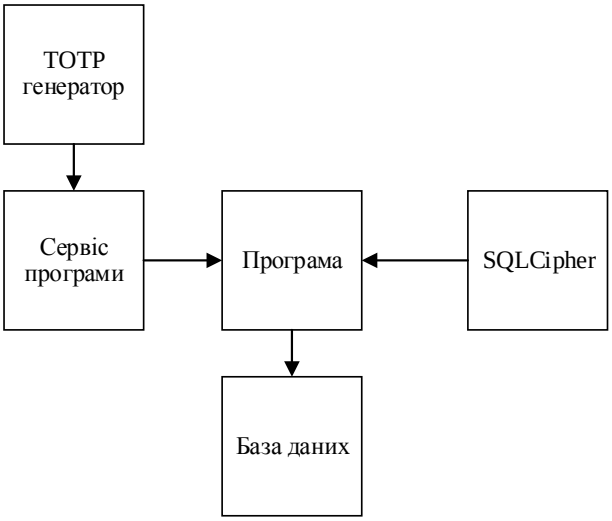

Рисунок 1 – Базова схема роботи додатку

Крім того, запропоновано забезпечити можливість очищення бази даних віддалено, що може стати у нагоді у випадках, коли мобільний пристрій викрадений, або загублений. Для цього пропонується використовувати технологію пуш-нотифікації, при отриманні якої буде проведено очищення даних програмного засобу. Цей метод дозволить певним чином захистити свої персональні дані у разі втрати мобільного пристрою.

Отже, запропоновано декілька методів захисту персональних даних користувача у мобільних пристроях, які працюють під управлінням операційної системи Android. Обґрунтовано їхню доцільність та економічність застосування. Продемонстровано основну ідею роботи програмного засобу.

Список використаних джерел

1. TOTP: Time-Based One-Time Password Algorithm [Електронний ресурс]. – Режим доступу: URL https://tools.ietf.org/html/rfc6238 - Назва з екрану.
2. SQLCipher: Encrypted Database [Електронний ресурс]. – Режим доступу: URL https://guardianproject.info/code/sqlcipher/- Назва з екрану.
3. Advanced Encryption Standard (AES) [Електронний ресурс]. – Режим доступу: URL http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard - Назва з екрану.

Гайдаєнко Олег Миколайович, факультет інформаційних технологій так комп'ютерної інженерії, група БС-12 б, Вінницький національний технічний університет, Вінниця, gaydayenko.o@gmail.com

Науковий керівник: ***Каплун Валентина Аполінаріївна,*** ст. викл. кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, valuka8379@gmail.com

Haydayenko Oleh Mykolayovych, Faculty of Information Technology and Computer Engineering, group BS-14в, Vinnytsia National Technical University, Vinnytsia, gaydayenko.o@gmail.com

Supervisor: ***Valentyna A. Kaplun*** — Lecturer of the Chair of Safety of Infomation and Communication Systems, Vinnytsia National Technical University, Vinnytsia, valuka8379@gmail.com