УДК 004.056.5

Артоуз А. О.

Городецька О. С.

Захист баз даних в операційній системі Android

Вінницький національний технічний університет

Анотація

Проаналізовано методи та засоби захисту баз даних від загроз, характерних для пристроїв з операційною системою Android.

Ключові слова: база даних, захист даних, SQL, Android.

Abstract

Methods and means of protecting databases from threats specific to devices with the Android operating system are analyzed.

Keywords: database, data protection, SQL, Android.

Вступ

У сучасному світі вирішення проблем раціонального використання актуальних методів і засобів обробки інформації має одне з найважливих значень в професійній діяльності в багатьох сферах. Розвиваються технічні та програмні засоби, що дозволяють реалізувати нові технології при прийнятному використанні ресурсів. Все більшої актуальності і широке поширення набувають бази даних (БД) і системи управління базами даних (СУБД), які використовуються для обробки великих обсягів різного роду інформації, в тому числі технічної, економічної тощо. БД здатні зберігати інформацію про десятки, сотні тисяч і мільйони різних об'єктів. Найбільші сучасні БД можуть обробляти обсяги інформації до декількох петабайт [1].

База даних - це сукупність даних, яка організована відповідно до певних правил і підтримується в пам'яті комп'ютера та характеризує актуальний стан деякої предметної області. Предметною областю є той фрагмент реального світу, чию інформацію потрібно зберігати і використовувати в конкретній задачі, що розв'язується в певному виді діяльності людини [2]. Головною перевагою використання БД можна назвати високу швидкість і ефективність пошуку з них необхідної інформації, час отримання якої мало залежить від загального обсягу зберігаються в базі даних.

Одним з найбільш актуальних питань є питання захисту даних в БД. Дослідимо методи захисту даних в операційній системі Android. Адже саме Android беззаперечно домінує на планеті, займаючи приблизно 74% світового ринку мобільних ОС. Найбільш перспективними методами захисту є хешування та шифрування.

Хеш-функція, або геш-функція — функція, що перетворює вхідні дані будь-якого (як правило великого) розміру в дані фіксованого розміру.

Хеш-функції пов'язані (і їх часто плутають) з контрольною сумою, контрольними цифрами, відбитками пальців, рандомізацією функцій, кодами, що виправляють помилки, і з шифрами. Хоча ці поняття певною мірою збігаються, кожен з них має свою власну область застосування і вимоги і є розробленим і оптимізованим по-різному[3].

Хешування застосовується для побудови асоціативних масивів, пошуку дублікатів в серіях наборів даних, побудови унікальних ідентифікаторів для наборів даних, контрольного підсумовування з метою виявлення випадкових або навмисних помилок при зберіганні або передачі, для зберігання паролів в системах захисту (у цьому випадку доступ до області пам'яті, де знаходяться паролі, не дозволяє відновити

сам пароль), при виробленні електронного підпису (на практиці часто підписується не саме повідомлення, а його геш-образ).

Шифрування — оборотне перетворення даних, з метою приховання інформації. Шифрування з'явилось близько 4 тисячів років тому.

Симетричне шифрування - це саме те, що ми використовуємо в більшості випадків, коли хочемо зашифрувати купу даних. Ваш браузер відправляє і отримує дані, використовуючи симетричне шифрування. Якщо ви шифруєте файли або диск, в цьому випадку теж працює симетричне шифрування. iMessage, Signal, WhatsApp - всі вони використовують симетричне шифрування для безпеки вашої переписки[4].

В асиметричному шифруванні дані шифруються одним ключем, а розшифровуються іншим. Перший ключ можна тримати у всіх на виду, а ось другий потрібно ховати.

Такий підхід знімає деякі питання безпеки в інтернеті: адже неможливо взагалі не передавати нікому ніякі ключі. Асиметричне шифрування допомагає з цим: частина ключів можна безпечно пересилати, це не порушить секретності.

Висновки

У роботі розглянуто особливості сучасних технологій для розробки мобільних додатків під Android. Було обране середовище Android Studio для розробки додатку, а використання бази даних допомагає зберегти всі необхідні користувачу дані. Найбільш розрповсюдженими методами захисту даних є хешування та шифрування у ОС Android. Такий підхід може значно зменшити ймовірність загрози таких порушень, як доступність, забезпечити цілісність та конфіденційність даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Реляційні бази даних для Android. [Електронний ресурс]: - Режим доступу: https://studwood.ru/1646246/informatika/relyatsiyni_bazi_danih_android
2. Медникс З., Дорнин Л., Мик Б., Накамура М. П78 Программирование под Android. 2-е изд. — СПб.: Питер, 2013. — 560 с.: ил. — (Серия «Бестселлеры O'Reilly»).
3. Защита данных в Android приложении. [Електронний ресурс]: - Режим доступу: https://jetruby.com/ru/blog/zaschita-dannyh-v-android/
4. Мохова, А. С. Особливості застосування баз даних і систем управління базами даних в економічній сфері / А. С. Мохова, М. Ю. Модулева. - Текст: безпосередній // Молодий вчений. - 2019. - № 52 (290). - С. 13-17. - URL: https://moluch.ru/archive/290/65915/ (дата звернення: 06.03.2021).

Артоуз Анастасія Олександрівна- студентка групи 2КІ-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: artouznastia13@gmail.com

Городецька Оксана Степанівна – кандидат технічних наук, доцент кафедри обчислювальної техніки Вінницького національного технічного університету, Вінниця, e-mail: gorodeczka.o.s@vntu.edu.ua

Artouz Anastasia – student of the 2KI-18b group, Faculty of Information Technologies and Computer Engineering, Vinnitsa National Technical University, Vinnitsa, e-mail: artouznastia13@gmail.com

Horodetska Oksana – Candidate of Technical Sciences, Associate Professor of the Department of Computer Science, Vinnitsa National Technical University, Vinnitsa, e-mail: gorodeczka.o.s@vntu.edu.ua