УДК 004.056.5:316.472.4

ОСОБЛИВОСТІ ПРОВЕДЕННЯ КРИМІНАЛІСТИЧНИХ ДОСЛІДЖЕНЬ МЕСЕНДЖЕРІВ В ОПЕРАЦІЙНІЙ СИСТЕМІ ANDROID

Рєзніченко Д.Ю.
e-mail: dymytrii.rieznichenko@nure.ua
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна

This work reveals the peculiarities and possible challenges in conducting digital forensic research on modern messengers in the Android operating system. Accordingly, the article describes the security mechanisms used in the Android operating system to protect the personal data (so-called artefacts) of messenger users, as well as the tools and methods that can be used to circumvent them (security mechanisms).

The paper also discusses how some popular messengers (including WhatsApp, Viber, Telegram, and Signal) use the security mechanisms built into Android.

Сучасні месенджери стали основним каналом спілкування для великої кількості людей з різних сфер життєдіяльності. Саме тому не є рідкістю випадки, коли ці програмні додатки використовуються для організації, координації та вчинення злочинів. У таких випадках, коли правоохоронним органам вдається відслідкувати та заарештувати зловмисників, то одним із основних предметів, який потенційно використовується для доказу вини підозрюваного, є його мобільний пристрій та інформація, яка у ньому зберігається.

Мобільні пристрої з операційною системою Android є дуже поширеними завдяки відкритості та доступності власної файлової системи, а також можливості вільно налаштовувати будь-яке встановлене на них програмне забезпечення. Але, з метою захисту конфіденційних та чутливих як користувацьких, так і системних даних, операційна система Android, за замовчуванням, надає користувачу лише необхідні для виконання базових операцій права доступу (тобто використовується принцип «найменших привілей»). Таким чином, доступ користувача обмежується до таких важливих системних директорій, як «/data/data/» та «/data/misc/keystore», які є основним сховищем технічних даних мобільних додатків, а також найбільшим місцем накопичення раніше згаданих артефактів.

У деякі мобільні пристрої, як додаткова міра безпеки, встановлюється також Hardware Security Module (HSM), який реалізований в Android у вигляді системи безпеки «Android Keystore» та використовується операційною системою як безпечне апаратне сховище криптографічних ключів [1].

Обидва вищезазначені механізми є основною точкою інтересу, яка з одного боку захищає дані користувача від несанкціонованого витоку, а з іншого – ускладнює будь-які процеси, пов'язані із криміналістичним дослідженням артефактів месенджерів. Але, варто зазначити, що описані вище механізми безпеки не є ідеальними, тому далі буде розглянуто існуючі методи їх обходу.

Як вже було сказано трохи вище, для цифрових криміналістів основними точками інтересу в операційній системі Android є приховані системні директорії «/data/data/» та «/data/misc/keystore». Переглянути вміст даних директорій можливо лише за наявності прав супер-користувача (тобто root-прав). І хоча сам процес отримання root-прав за останні роки став доволі простим у реалізації та автоматизованим (наприклад, можна використати добре відомі інструменти «Magisk» або «KingoRoot»), але він іноді може спричинити наступні наслідки: пошкодження файлової системи, видалення персональної інформації користувача та інше. Таким чином, важливі артефакти, під час процесу отримання root-прав, можуть бути випадково видалені.

У вищезазначеному випадку, рішенням проблеми може стати використання таких інструментів, як «Shizuku» [2] у комбінації із будь-яким стороннім (не вбудованим в операційну систему) файловим провідником (наприклад, «Solid Explorer» від NeatBytes) [3]. Так, за допомогою Shizuku можна налаштовати окремий сервер, який дозволяє використовувати Android Debug Bridge (ADB) для прямої взаємодії із системними процесами та компонентами. Також, якщо даний Shizuku-сервер налаштувати в будь-якому сторонньому файловому провіднику як основний канал комунікації із мобільним пристроєм, то з'явиться можливість створювати, копіювати і видаляти файли у системних директоріях. Особливістю вищеописаного рішення є можливість безпечно вилучити артефакти з мобільного пристрою.

Якщо ж говорити про HSM, то тут ситуація трохи складніша. Загалом, даний модуль використовується деякими месенджерами (наприклад, Signal Messenger) для створення та зберігання криптографічних ключів. У випадку із Signal Messenger, вищезазначені криптографічні ключі (які існують у вигляді файлу «USRPKEY_SignalSecret») потім використовуються для шифрування/розшифрування бази даних «signal.db» у директорії «/data/data/org.thoughtcrime.securesms/databases».

Взаємодія месенджерів із модулем HSM відбувається через відповідні Application Programming Interface (API). За допомогою API, месенджери мають можливість створювати криптографічні ключі, зберігати їх до HSM, читати їх вміст, а також видаляти. Особливістю HSM є те, що будь-який криптографічний секрет, який був завантажений до нього, неможливо вилучити [1].

Але, у модуля HSM є наступна вразливість: якщо операційна система мобільного пристрою, де існує HSM, скомпрометована, то зловмисник має

можливість, використовуючи відповідні API, прочитати криптографічні ключі [1].

Як вже було зазначено вище, основною робочою директорією модуля HSM в операційній системі Android є «/data/misc/keystore». Її вміст можна побачити на рисунку 1.

```
:/data/misc/keystore/user_0 # ls
10008_USRCERT_c5635988b7157a3a
10008_USRCERT_unstable+^825349ac930c2370b39f30e7d789963b+^2
10008_USRPKEY_c5635988b7157a3a
10008_USRPKEY_unstable+^825349ac930c2370b39f30e7d789963b+^2
10033_USRPKEY_gmphn_pkey
10076_CACERT_the_well_of_wishes_awaits_in_the_crypt_of_decay_86a4aeec+]b2f3+]4bda+]ac87+]86af56b403aa
10076_USRCERT_the_well_of_wishes_awaits_in_the_crypt_of_decay_86a4aeec+]b2f3+]4bda+]ac87+]86af56b403aa
10076_USRPKEY_aes_auth_key
10076_USRPKEY_the_well_of_wishes_awaits_in_the_crypt_of_decay_86a4aeec+]b2f3+]4bda+]ac87+]86af56b403aa
10078_USRPKEY_SignalSecret
10080_USRPKEY_key2
:/data/misc/keystore/user_0 #
```

Рисунок 1 – Вміст робочої директорії системи «Android Keystore»

На рисунку 1 можна побачити перелік файлів у директорії «/data/misc/keystore», які містять криптографічні секрети різних користувацьких і системних додатків та(або) компонентів. Для отримання доступу до вищезазначеної директорії, було створено віртуальну машину у середовищі VirtualBox з операційною системою Android 9.0 R2, яка вже має активовані root-права для користувача.

Наостанок необхідно розглянути, як інші месенджери (такі як WhatsApp, Viber та Telegram) використовують механізми безпеки Android. Загалом, месенджери Telegram, WhatsApp та Viber зберігають будь-які артефакти у адміністративній директорії «/data/data/». У випадку із Viber та WhatsApp, їх артефакти зберігаються у вищезазначеній директорії у незашифрованому вигляді. Це означає, що, за наявності root-прав, користувач може безперешкодно працювати із базами даних цих месенджерів (наприклад, переглядати їх вміст через SQLite Editor). Також, на відміну від месенджера Signal, WhatsApp зберігає власні криптографічні ключі не в HSM, а в директорії «/data/data/com.whatsapp/shared_prefs» у файлі «keystore.xml», що спрощує процес їх вилучення.

Месенджер Telegram, хоч і не зберігає персональну інформацію користувача на його мобільному пристрої, але в адміністративній директорії «/data/data/org.telegram.messenger/files» створює незашифровану базу даних «cache4.db», яка містить у собі кеш текстових повідомлень, списку контактів суб’єкта та інше.

Список використаних джерел:

1. Android Keystore system : вебсайт. URL: https://developer.android.com/privacy-and-security/keystore#SecurityFeatures (дата звернення: 28.02.2025).

2. Shizuku // GitHub. URL: https://github.com/RikkaApps/Shizuku (дата звернення: 02.03.2025).

3. Android 14 How to Access Android Data & OBB Folders // YouTube. URL: https://youtu.be/e1GIAtT5USw?si=ghFJw1Vqjg0xGgXd (дата звернення: 04.03.2025).