АНАЛІЗ ШИФРУВАННЯ ДАНИХ У СМАРТФОНАХ ПОПУЛЯРНИХ КИТАЙСЬКИХ ВИРОБНИКІВ

Султанов Д. Д., Данилов А. Д.
Харківський національний університет радіоелектроніки, Харків, Україна

Відомо, що багато жителів Європи та Азії надає перевагу смартфонам китайських виробників. Більша частина ринку усіх смартфонів у цих регіонах носять ім'я одного з найбільших китайських брендів, таких як Xiaomi чи Huawei. Але чи є достатньо надійними їх внутрішні служби передачі даних [1]? Розглянемо ситуацію на прикладі найпопулярнішого виробника смартфонів із піднебесної – компанії Xiaomi.

Ряд системних програм спочатку шифрують дані за допомогою AES/ECB/CBC при передачі за допомогою SSL-з'єднання. Програма Analytics (com.miui.analytics) надсилає телеметрію на сервер tracking.intl.miui.com. Протокол обміну ключами включає генерацію телефоном випадкового 128-бітного AES-ключа, потім шифрує його за допомогою відкритого ключа RSA і передає в кодуванні base64 на сервер. У відповідь сервер надсилає другий ключ AES, зашифрований за допомогою першого, а також значення SID для ідентифікації ключа, використаного для шифрування [2]. Телефон розшифровує отриманий ключ, генерує ключову пару RSA та використовує відкритий ключ для шифрування ключа AES перед збереженням на диску як дані SharedPreference. Оскільки закритий ключ RSA зберігається в захищеному елементі, він доступний лише програмі. Тобто ключ AES ніколи не буде незашифрований у стані спокою. Аналогічний протокол обміну ключами використовується й іншими системними програмами Xiaomi. Зокрема, програма MSA (com.miui.msa.global) надсилає зашифровані дані на сервер api.ad.intl.xiaomi.com, який, мабуть, пов'язаний з керуванням рекламою. Інші вбудовані програми, як Mi File Explorer (com.mi.android.globalFileexplorer), Mi Settings (com.xiaomi.misettings) і програма Xiaomi Security (com.miui. securitycenter), використовують аналогічний підхід для шифрування даних [3].

Виходячи з вищенаведених даних, можемо побачити, що смартфони Xiaomi мають достатній рівень захисту персональних даних користувача при передачі їх на свої сервери.

Список літератури

1. Сєвєрінов О. В., Федорченко В. М., Перепадя В. І. Аналіз загроз персональним даним в мобільному пристрої під час використання різноманітних додатків / Системи озброєння і військова техніка 4 (2016): 42-45.
2. L. Sweeney, "k-anonymity: A model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 05, pp. 557–570, 2020.
3. D. J. Leith, "Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google," in Proc Securecomm, 2021.