ШИФРОВАНИЕ ДАННЫХ В ОПЕРАЦИОННОЙ СИСТЕМЕ ANDROID С JETPACK SECURITY

Якимович Алексей Владимирович
магистрант, Белорусский государственный университет информатики и радиоэлектроники, Беларусь, г. Минск
E-mail: yaki.alex123@gmail.com

Прохоренко Артём Сергеевич
магистрант, Белорусский государственный университет информатики и радиоэлектроники, Беларусь, г. Минск
E-mail: acprohor@gmail.com

Для обеспечения безопасности начиная с Android 5 (SDK 21) [1] система может шифровать содержимое раздела пользовательский данных. Но в некоторых случаях могут понадобятся дополнительные меры защиты. Например, если приложение использует общее хранилище и вам необходимо зашифровывать некоторые данные. Для таких ситуаций вызвана помочь крипто-библиотека Jetpack Security (JetSec).

Jetpack Security (JetSec) — это крипто-библиотека которая предоставляет абстракции для шифрования таких объектов как файлы и SharedPreferences. Библиотека продвигает использования AndroidKeyStore с использованием безопасных и известных криптографических примитивов. Использование EncryptedFile и EncryptedSharedPreferences позволяет локально защитить файлы, которые могут содержать конфиденциальные данные, ключи API, токены OAuth и другие типы секретов [2].

Стоит отметить для чего в системе нужен AndroidKeyStore. Система Android Keystore позволяет хранить криптографические ключи в так называемом контейнере, для того чтобы его было сложнее извлечь из устройства. Как только ключи находятся в хранилище ключей их можно использовать для криптографических операций, при этом сам ключ остается не экспортируемым. Кроме того, он дает возможные средства для ограничения того, как и когда могу использоваться ключи [3].

Jetpack Security основан на Tink [4], кроссплатформенном проекте безопасности с открытым исходным кодом от Google. Tink может подойти, если вашему приложению нужно общее шифрование или гибридное шифрование. Структуры данных Jetpack Security полностью совместимы с Tink.

Генерация ключей

Jetpack Security использует главный ключ, который шифрует все подключи, которые используются для каждой криптографической операции. JetSec предоставляет рекомендуемый мастер-ключ по умолчанию в классе MasterKeys. В этом классе используется базовый ключ AES256-GCM, который создается и хранится в AndroidKeyStore. В AndroidKeyStore криптографические ключи хранятся в TEE или StrongBox, что затрудняет их извлечение. Подключи хранятся в настраиваемом объекте SharedPreferences.

В Jetpack Security в первую очередь используется спецификация AES256_GCM_SPEC, которая рекомендуется для общих случаев использования. AES256-GCM является симметричным и в целом быстрым на современных устройствах. Для приложений, которые требуют большей конфигурации или обрабатывают очень конфиденциальные данные, рекомендуется создать KeyGenParameterSpec. Ключи с привязкой по времени с BiometricPrompt могут обеспечить дополнительный уровень защиты.

Шифрование файлов

Jetpack Security включает класс EncryptedFile, который устраняет проблемы, связанные с шифрованием файлов. Подобно File, EncryptedFile предоставляет объект FileInputStream

для чтения и объект FileOutputStream для записи. Файлы шифруются с использованием потоковой передачи AEAD, которая соответствует определению OAE2 [5]. Данные делятся на куски и шифруются с использованием AES256-GCM таким образом, что невозможно изменить порядок.

Шифрование SharedPreferences

Если приложению необходимо сохранить пары ключ-значение, например, ключи API — это JetSec предоставляет класс EncryptedSharedPreferences, который использует тот же интерфейс SharedPreferences.

И ключи, и значения зашифрованы. Ключи зашифрованы с использованием AES256-SIV-CMAC, который обеспечивает детерминированный зашифрованный текст; значения зашифрованы с помощью AES256-GCM и привязаны к зашифрованному ключу. Эта схема позволяет безопасно шифровать данные ключа, в то же время разрешая поиск.

Заключение.

Рассмотрев основные принципы данной крипто-библиотеки, можно сказать, что Jetpack Security является хорошим и гибким инструментом призванным улучшить безопасность в операционной системе Android.

Список литературы:

1. Страница, посвящённая шифрованию в операционной системе Android [Электронный ресурс]. —Режим доступа https://source.android.com/security/encryption . — 17.04.2020.
2. Шифрование данных на Android с Jetpack Security [Электронный ресурс]. —Режим доступа: https://android-developers.googleblog.com/2020/02/data-encryption-on-android-with-jetpack.html. — 17.04.2020.
3. Система хранения ключей в операционной системе Android [Электронный ресурс]. — Режим доступа: https://developer.android.com/training/articles/keystore. — 17.04.2020.
4. Открытый исходный код Tink [Электронный ресурс]. —Режим доступа: https://github.com/google/tink. — 17.04.2020.
5. Описание AEAD [Электронный ресурс]. —Режим доступа: https://github.com/google/tink/blob/master/docs/PRIMITIVES.md#streaming-authenticated-encryption-with-associated-data. — 17.04.2020.