Исследование шифрования данных приложения Wickr для различных платформ

Чернявский Олег, 17.Б11-мм

Научный руководитель: Литвинов Юрий Викторович

Консультант: Тимофеев Никита Михайлович, ООО “Belkasoft”

Мотивация

- **Wickr** является одной из наиболее защищенных платформ для коммуникации
- В ее экосистему входит приложение **Wickr Me** — анонимный мессенджер с полным шифрованием данных
- Преимуществами **Wickr Me** могут воспользоваться и преступники, желающие скрыть следы своей незаконной деятельности
- По этой причине доступ к данным, хранимым **Wickr Me** на конечных устройствах, представляет особенный интерес для экспертов в сфере цифровой криминалистики

Цели и задачи

Цель: методами реверс-инжиниринга исследовать алгоритмы шифрования хранимых приложением данных и реализовать их расшифровку. Целевые платформы: iOS и Android.

Задачи:

- Описать структуру хранимых приложением данных
- Определить используемые алгоритмы шифрования и их параметры
- Описать способ извлечения ключей шифрования данных Wickr Me
- Описать механизм расшифровки данных приложения
- Интегрировать механизм расшифровки данных в Belkasoft X

Существующие решения

Продукт	Поддерживаемые платформы	Является ли ПО проприетарным	Есть ли открытое описание принципа работы
Cellebrite Responder	iOS, Android	**Да**	**Нет**
Magnet AXIOM	iOS	**Да**	**Нет**
Oxygen Forensic Detective	Android	**Да**	**Нет**
XRY	Android	**Да**	**Нет**

Таблица 1: ПО, поддерживающее извлечение данных из Wickr Me

Версия Wickr Me для iOS. Данные приложения

- Данные приложения хранятся в директории **private/var/mobile/Containers/Shared/AppGroup**
- Сам файл базы данных **не зашифрован**, часть информации (например, время отправления сообщения) доступна сразу
- Текст сообщений хранится в колонке ZBODY таблицы ZWICKR_MESSAGE и **зашифрован**
- Информация о прикрепленных к сообщению файлах хранится в таблицах ZWICKR_FILE и Z_11MSG
- Сами файлы находятся в директории **private/var/mobile/Containers/Data/Application** в зашифрованном виде

Версия Wickr Me для iOS. Расшифровка ключей шифрования данных без пароля пользователя

- Расшифровка происходит в два этапа с помощью алгоритма **AES-256** в режиме **Galois/Counter Mode (GCM)**
- На первом этапе в качестве зашифрованного значения используется значение **zph** из таблицы ZSECEX_ACCOUNT, а в роли ключа выступает комбинация **BundleID** и значения **!devID!** из iOS Keychain
    - **BundleID** — уникальный идентификатор iOS-приложения (для Wickr Me — com.mywickr.wickr)
- На втором этапе в качестве ключа используется значение **activeAccount** из iOS Keychain
- Результат — protobuf-сообщение, содержащее **ключ шифрования** значений из базы данных

Версия Wickr Me для iOS. Расшифровка ключей шифрования данных по паролю пользователя

- Расшифровка происходит в два этапа, первый — с помощью криптографической функции **Scrypt**, второй — алгоритма **AES-256** в режиме GCM
- На первом этапе с помощью криптографической функции **Scrypt** по **паролю пользователя** и 16 байтам значения **zpt** из таблицы ZSECEX_ACCOUNT формируется ключ шифрования для следующего раунда
- Далее, используя полученный ключ, оставшиеся байты **zpt** расшифровываются с помощью алгоритма **AES-256-GCM**
- Результат — точно такое же protobuf-сообщение, что и в предыдущем методе

Версия Wickr Me для iOS. Расшифровка хранимых данных

- Зашифрованные данные в БД можно расшифровать с помощью **полученного ключа** и алгоритма **AES-256** в режиме GCM
- Данные о переписке (текст, геолокация, информация о приложенных файлах) хранятся в **protobuf-сообщениях**
- Приложенные к сообщением файлы также зашифрованы с помощью **AES-256-GCM**, ключи шифрования содержаться в зашифрованных данных в базе

Версия Wickr Me для Android. Данные приложения

- Данные приложения хранятся в директории **/data/data/datacom.mywickr.wickr2**
- Файл базы данных **wickr_db** хранится в поддиректории “databases” и полностью зашифрован
- База данных содержит **пользовательскую информацию** (имена пользователя и его контактов, их идентификаторы, публичные и приватные ключи и т.д.) и переписку
- Приложенные к сообщениям файлы хранятся в поддиректории **files/enc** в зашифрованном виде

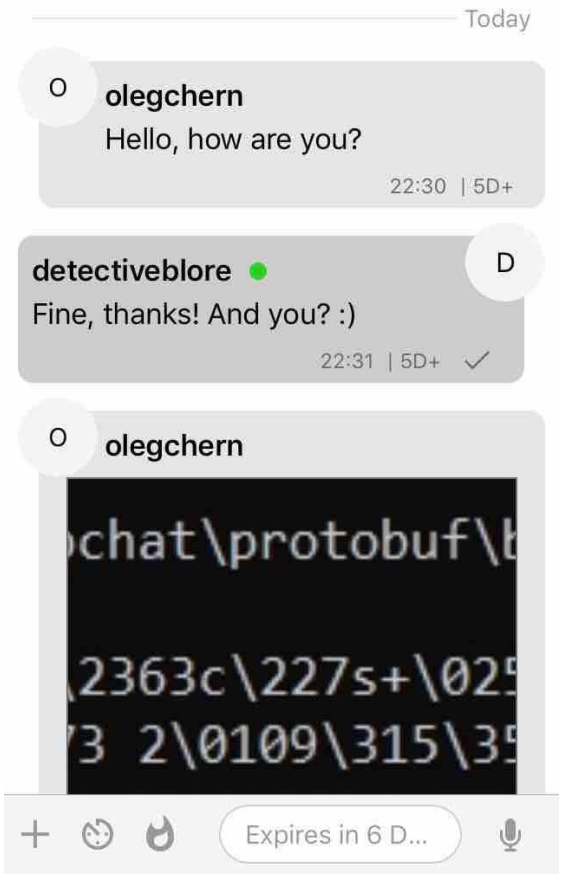
Версия Wickr Me для Android. Расшифровка ключей шифрования

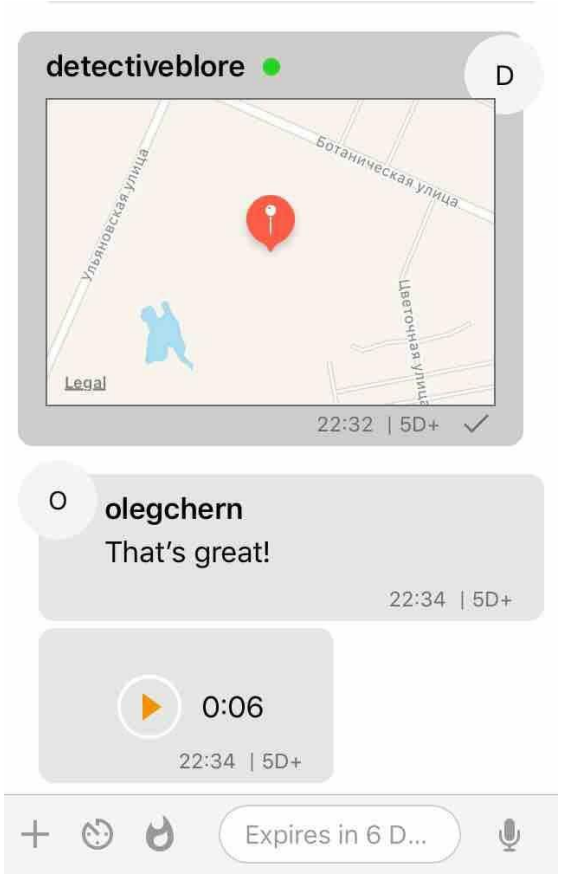
- Механизмы расшифровки данных в версии для **Android** крайне похожи на механизмы в версии для **iOS**
- Расшифровка без пароля пользователя проходит аналогичным образом в два этапа с помощью **AES-256-GCM**
  - На первом этапе зашифрованное значение берется из файла **kcd.wic**, а ключом является системное значение **android_id**
  - На втором этапе в роли ключа выступает содержимое файла **kck.wic**
- Расшифровка по паролю пользователя также проходит в два этапа с использованием **Scrypt** и **AES-256-GCM**
  - Соль для первого этапа и зашифрованное значение для второго берутся из файла **sk.wic**

Версия Wickr Me для Android. Расшифровка хранимых данных

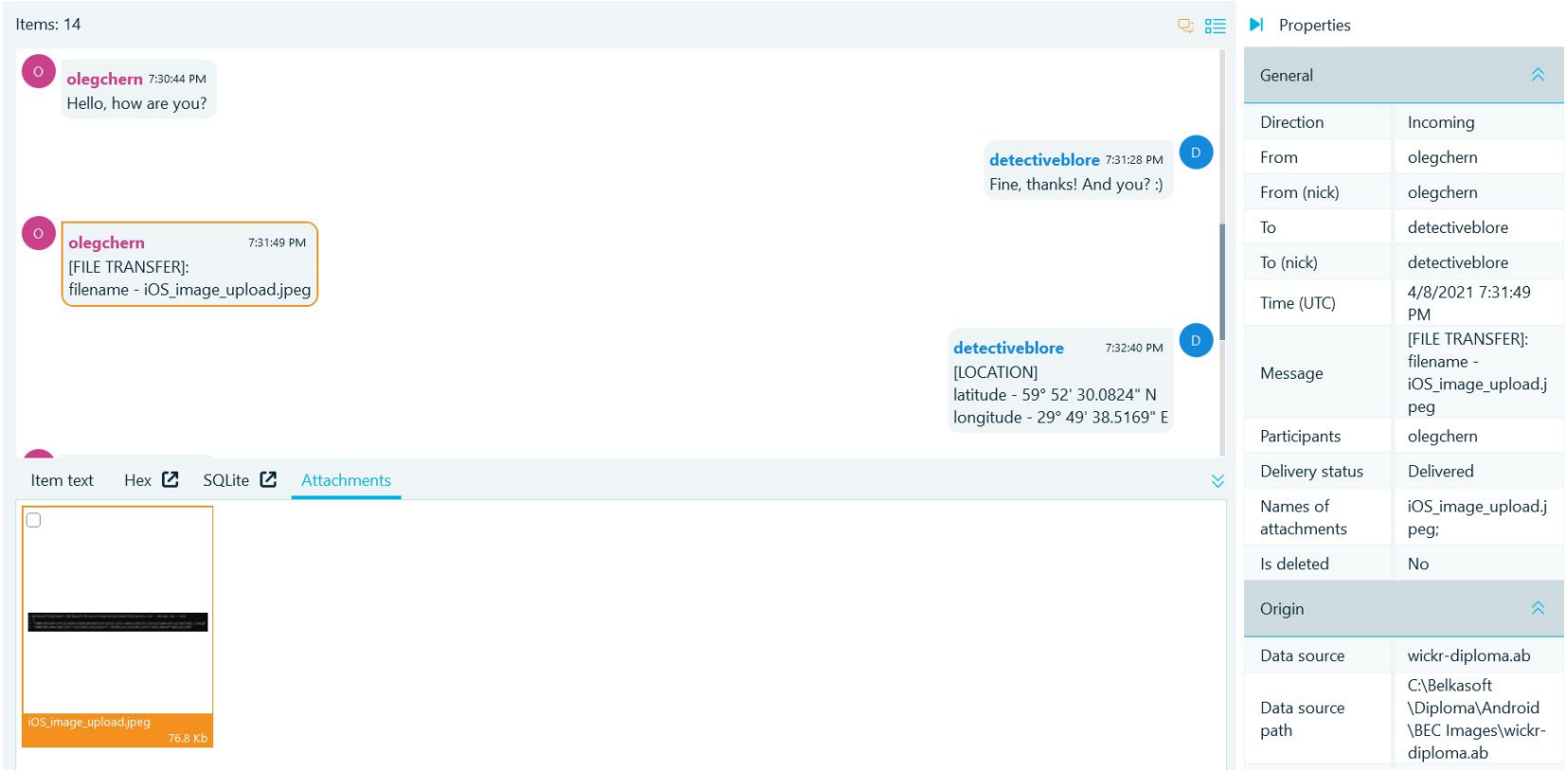
- В результате использования этих методов получаем такое же **protobuf-сообщение**, что и в версии для iOS
- База данных зашифрована с помощью библиотеки **SQLCipher**, пароль — извлеченный ключ в формате hex-строки
- Устройство базы данных во многом повторяет структуру БД из версии для **iOS**
- Значения в БД и приложенные к сообщениям медиа-файлы зашифрованы с помощью алгоритма **AES-256** в режиме **GCM**

Внедрение результата в Belkasoft X





Внедрение результата в Belkasoft X



Результаты

- **Описана** структура хранимых приложением данных
- **Определены** используемые приложением алгоритмы шифрования и их параметры
- **Описан** способ получения ключей шифрования данных Wickr Me
- **Описан** механизм расшифровки данных приложения
- Механизм расшифровки данных Wickr Me **внедрен** в Belkasoft X