Рецензия на выпускную квалификационную работу студента Чернявского О.Н. на тему «Исследование шифрования данных приложения Wickr для различных платформ»

Рецензент – Ханов А.Р.

В работе рассматривается проблема извлечения данных программ из мобильных устройств. В качестве цели был выбран мессенджер Wickr.

Эта задача имеет высокую актуальность прежде всего для специалистов по расследованию компьютерных преступлений, которым приходится иметь дело со смартфонами, на которых установлено это приложение. Схожий функционал был встроен в ряд коммерческих продуктов, однако сообществу исследователей не был известен алгоритм, с помощью которого происходит извлечение данных (вендоры тщательно берегут свои секреты).

В качестве исходных данных студент использовал смартфоны iPhone 5S и Xiaomi Mi5 с установленными приложениями, а также тестовый аккаунт. Проблема была в том, что базы данных мессенджера хранятся в зашифрованном виде. Это сделано для их защиты от возможной кражи, но затрудняет работу в случае необходимости их легального извлечения.

В работе проанализированы приложения для iOS и Android. В начале изучался набор файлов приложений и производился поиск базы данных. Оказалось, что информация о сообщениях пользователя частично зашифрована. Доступна лишь метаинформация, а тела сообщений и вложения зашифрована неизвестным ключом. Кроме того, в версии для Android зашифрована и сама база данных.

Для выявления алгоритма формирования этого ключа, а также алгоритма расшифровки отдельных сообщений в базе и самой базы данных (для Android) был произведен реверс-инжиниринг приложений.

Для приложения iOS было проведено снятие дампа с помощью утилиты Frida, что дало возможность пользоваться не только статическим анализом кода, но и видеть константы рантайма. Студент проанализировал граф потока управления и нашел алгоритм формирования ключа по кешу ключей, а также по паролю пользователя. В работе приведено описание каждого шага, приведены декомпилированные коды функций и форматы хранимых в программе данных. Оказалось, что ключ формируется из фиксированной строчки и значения, хранимого в хранилище ключей iOS. Помимо этого, возможно расшифровать ключ, шифрующий сообщения, зная пароль пользователя.

В результате работы был полностью декомпилирован алгоритм шифрования сообщений данного приложения. Более того, работа получила апробацию и реально промышленное внедрение и является частью приложения Belkasoft X.

Работа не лишена недостатков:

1. Главный вопрос – научная ценность работы и отчуждаемость результата. Будь у нас исходный код/документация приложения, или исходный код/документация от различных утилит анализа, то задача бы сильно упростилась. Однако в большинстве работ по реверс-инжинирингу специалисты сталкиваются именно с проблемой отсутствия или неполноты информации об исследуемом объекте и

решают поставленную задачу в таких условиях. Отчуждаемость результата также имеет место – любой специалист, который ознакомится с работой, сможет применить знания на практике.

2. Стоит обеспечить читателю, не знакомому с проблематикой данной области, почему нельзя просто включить приложение и прочитать все сообщения, заставив приложение расшифровать данные из базы
3. В целях более понятного описания алгоритма работы стоит привести его схему, на которой показать потоки данных и те места, из которых берутся данные для формирования и расшифровки ключей.

Рекомендуемая оценка – отлично.