

Рецензия на выпускную квалификационную работу студента Афанасова А.К. на тему «Извлечение данных Android-приложения WhatsApp»

Рецензент – Ханов А.Р.

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

Студентом был проведен обзор, согласно которому данная задача решалась несколькими исследователями, но до конца так и не была решена. Основной результат работы – реверс и реализация алгоритма получения резервных копий с сервера WhatsApp без участия официального приложения. Это было достигнуто путем реверса и модификации iOS версии приложения, а также благодаря мониторингу трафика через Wireshark.

Работа имеет важное прикладное значение. Авторы утилит по извлечению данных с устройств могут использовать данный алгоритм для работы с Whatsapp, разработчикам самого приложения это поможет улучшить защиту от извлечения данных. Работа получила апробацию и реально промышленное внедрение и является частью приложения Belkasoft X. Подробно описана архитектура реализованного прототипа.

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

Студент продемонстрировал высокий уровень владения инструментами статического и динамического реверс-инжиниринга программ, средствами анализа трафика, знание алгоритмов криптографии, умение анализировать работу программ.

Рекомендуемая оценка – отлично.