DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.1.5

УДК 004.9
ББК 32.973-012

АСПЕКТЫ АНАЛИЗА ЗАЩИЩЕННОСТИ И УЯЗВИМОСТЕЙ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Александр Самвелович Макарян

Кандидат технических наук,
старший преподаватель кафедры компьютерных технологий и информационной безопасности,
Кубанский государственный технологический университет
msanya@yandex.ru
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

Михаил Александрович Карманов

Студент,
Кубанский государственный технологический университет
michaelKdev15@gmail.com
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

Аннотация. В рамках данной работы были рассмотрены варианты реализации защиты локальных данных приложений на мобильных устройствах, имеющих операционные системы Android и iOS. В качестве исследуемых программ были выбраны следующие: мессенджеры WhatsApp, Viber, Telegram, WeChat, Signal. В ходе анализа были определены и классифицированы хранимые в приложениях локальные данные. В качестве результатов были получены данные об имеющихся в программах механизмах защиты, хранимых типах данных, потребовавшихся инструментах и технологиях, а также предположения по улучшению защиты хранимых локальных данных программ.

Ключевые слова: безопасность приложений, мобильные устройства, защита данных, анализ, уязвимости.

В качестве исследуемых приложений были выбраны следующие: мессенджеры WhatsApp, Viber, Telegram, WeChat и Signal. В случае с мессенджерами критичными данными считаются следующие типы данных: истории сообщений и вызовов, контактная информация об участниках чатов и диалогов, информация о ключах шифрования (мастер-ключ, ключ сессии и т. д.), а также вторичная информация (служебные журналы работы и другие источники, не участвующие в непосредственной работе приложения). Сравнительная характеристика защищенности мессенджера WhatsApp представлена на таблице 1.

Сравнительная характеристика защищенности мессенджера Viber представлена на таблице 2.

Сравнительная характеристика защищенности мессенджера Telegram представлена на таблице 3.

Сравнительная характеристика защищенности мессенджера WeChat представлена на таблице 4.

Сравнительная характеристика защищенности мессенджера Signal представлена на таблице 5.

Стоит отметить, что в популярных для нашей страны мессенджерах только в слу-

чае с мессенджером Telegram внедрено кодирование сообщений, которое может быть обойдено изучением декомпилированного исходного кода мессенджера. При исследовании полученного исходного кода данного мессенджера было установлено, что имеется, на момент исследования, 31 возможный протокол кодирования сообщений в базе данных. Без использования данной информации невозможно установить содержание сообщений чатов всех видов, хранящихся в базе данных [2].

Таблица 1

Сравнительная характеристика защищенности мессенджера WhatsApp

Доступность сообщений	Сообщения хранятся в открытом виде в msgstore.db (ChatStorage.sqlite для iOS)
Доступность контактной информации	Контактная информация хранится в открытом виде в wa.db (Contacts.sqlite для iOS)
Доступность ключевой информации	Мастер-ключ возможно получить из файла «key» для расшифровки инкрементных резервных копий историй сообщений
Вторичная информация	По журналам работы программы можно установить время и дату событий приложения
Инструменты и методы для обхода механизмов защиты	Apk signature expoit, создание резервной копии через Android Debug Bridge

Таблица 2

Сравнительная характеристика защищенности мессенджера Viber

Доступность сообщений	Сообщения хранятся в открытом виде в viber_messages (Contacts для iOS)
Доступность контактной информации	Контактная информация хранится в открытом виде в viber_data (Contacts для iOS)
Доступность ключевой информации	Информация о различных ключах отсуствует
Вторичная информация	Кодирование аудио- и видеосообщений пропритарным алгоритмом
Инструменты и методы для обхода механизмов защиты	Apk signature expoit, создание резервной копии через Android Debug Bridge; apktool + jdgui (декомпиляция исходного кода для получения алгоритма кодирования)

Таблица 3

Сравнительная характеристика защищенности мессенджера Telegram

Доступность сообщений	Сообщения хранятся в закодированном виде в cache4.db (в том числе и сообщения Secret-чатов)
Доступность контактной информации	Контакты хранятся в открытом виде в cache4.db
Доступность ключевой информации	Информация о различных ключах отсутствует
Вторичная информация	Критичной для исследования информации найдено не было
Инструменты и методы для обхода механизмов защиты	Apk signature expoit, создание резервной копии через Android Debug Bridge; apktool + jdgui (декомпиляция исходного кода для получения алгоритмов кодирования сообщений)

Таблица 4

Сравнительная характеристика защищенности мессенджера WeChat

Доступность сообщений	Сообщения хранятся в зашифрованной базе данных EnMicroMsg.db (в открытом виде в MM.db для iOS)
Доступность контактной информации	Контакты хранятся в зашифрованной базе данных EnMicroMsg.db (в открытом виде в MM.db для iOS)
Доступность ключевой информации	В конфигурационных файлах содержатся составные части ключа шифрования баз данных
Вторичная информация	Критичной для исследования информации найдено не было
Инструменты и методы для обхода механизмов защиты	Apk signature expoit, создание резервной копии через Android Debug Bridge; apktool + jdgui (декомпиляция исходного кода для получения алгоритма шифрования базы данных); sqlcipher (получение расшифрованной базы данных)

Таблица 5

Сравнительная характеристика защищенности мессенджера Signal

Доступность сообщений	Сообщения зашифрованы и хранятся в проприетарной кодировке в messages.db
Доступность контактов	Контакты хранятся в обезличенной форме в wisher_directory.db
Доступность ключевой информации	Составные части мастер-ключа, сессионные ключи хранятся в конфигурационных файлах в закодированном виде
Вторичная информация	В закрытой от пользователя директории хранятся зашифрованные вложения
Инструменты и методы для обхода механизмов защиты	Apk signature expoit, создание резервной копии через Android Debug Bridge; apktool + jdgui (декомпиляция исходного кода для получения алгоритма декодирования и шифрования сообщений, а также шифрования вложений)

При анализе мессенджера WeChat с помощью подхода декомпиляции и изучения исходного кода удалось извлечь алгоритм генерации мастер-ключа расшифровки базы данных: объединяются две строки – IMEI устройства и UID (уникальный идентификатор аккаунта в системе WeChat), для результата вычисляется хэш по алгоритму MD5, из которого берутся первые 8 символов как парольная фраза [1; 3]. Сама база данных шифруется по технологии SQLCipher. Используя сгенерированную парольную фразу и утилиту sqlcipher, предоставляющую функционал по работе с базами данных SQLite, зашифрованных по технологии SQLCipher, можно расшифровать базу данных и получить данные историй сообщений и контактных данных мессенджера. При анализе же на iOS (версии программы) база данных вообще не была зашифрована.

При изучении мессенджера Signal был применен схожий подход и был получен алгоритм генерации мастер-ключа, который является базисом для расшифровки каждого отдельно зашифрованного сообщения в базе данных, а также ключом для расшифровки вложений, зашифрованных по алгоритму AES-CBC со 128-битным ключом.

Как выяснилось в ходе данной работы, локально хранящимся программным данным на устройстве уделяется недостаточно внимания в плане защиты, так как в некоторых случаях данная защита построена исключительно на механизмах операционной системы устройства. Для более надежной защиты локально хранящихся данных приложения необходимо внедрить в приложение следующие подходы:

– шифрование как базы данных полностью, так и отдельных критичных данных в ней по отдельности дополнительным слоем шифрования;

– шифрование файлов, появляющихся в ходе выполнения программы (медиа-файлы, к примеру);

– кодирование и представление данных в программе с использованием проприетарных алгоритмов;

– использование запутывающих имен критичных файлов и данных (файл с ключом не стоит называть «key», как, например, в случае с WhatsApp), а также данных-ловушек;

– кодирование конфигурационных файлов, содержащих критичную информацию для обеспечения защищенности данных;

– вынесение функционала ядра криптографических преобразований в отдельную подключаемую библиотеку с целью сделать изучение декомпилированного исходного кода на предмет данных преобразований бессмысленным.

СПИСОК ЛИТЕРАТУРЫ

1. Anglano, C. Forensic Analysis of WhatsApp Messenger on Android Smartphones / C. Anglano // ResearchGate : [информационно-справочный портал]. – Electronic data. – Mode of access: https://www.researchgate.net/publication/262641460 (date of access: 10.02.2018). – Title from screen.

2. Current TL Schema // Telegram : [информационно-справочный сайт]. – Electronic data. – Mode of access: https://core.telegram.org/schema (date of access: 11.03.2018). – Title from screen.

3. Darus, F. M. How to decrypt WeChat EnMicroMsg.db database? / F. M. Darus // Forensic Focus. – Electronic data. – Mode of access: https://

articles.forensicfocus.com/2014/10/01/decrypt-wechat-enmicromsgdb-database/ (date of access: 21.03.2018). – Title from screen.

REFERENCES

1. Anglano C. *Forensic Analysis of WhatsApp Messenger on Android Smartphones*. URL: https://www.researchgate.net/publication/262641460 (accessed 10 February 2018).

2. *Current TL Schema*. URL: https://core.telegram.org/schema (accessed 11 March 2018).

3. Darus F.M. *How to decrypt WeChat EnMicroMsg.db database?* URL: https://articles.forensicfocus.com/2014/10/01/decrypt-wechat-enmicromsgdb-database/ (accessed 21 March 2018).

ASPECTS OF ANALYZING THE SECURITY AND VULNERABILITIES OF MOBILE APPLICATIONS

Aleksandr Samvelovich Makaryan

Candidate of Sciences (Engineering),
Senior Lecturer, Department of Computer Technologies and Information Security,
Kuban State Technological University
msanya@yandex.ru
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

Mikhail Aleksandrovich Karmanov

Student,
Kuban State Technological University
michaelKdev15@gmail.com
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

Abstract. The given article deals with the variants of mobile applications' local data protection on devices with operation systems Android and iOS. The following programs have been investigated: messengers WhatsApp, Viber, Telegram, WeChat, Signal. The conducted analysis let define and classify the programs for protection mechanisms, the types of stored data, the required tools and technologies, as well as the techniques for improving the protection of the stored local data.

As it turned out in the course of this research work, locally stored software data on the device is not given enough attention in terms of protection, as in some cases, this protection is based solely on the mechanisms of the operating system of the device. For more reliable protection of locally stored data of the application it is necessary to implement the following approaches in the application: encryption of both the database in full and some critical data in it separately by an additional layer of encryption; encryption of files that appear during the program execution (media files, for example); coding and representation of data in a program using proprietary algorithms; the use of confusing names of critical files and data (the key file should not be called "key", as in the case of WhatsApp), and data traps; the encoding of the configuration files containing sensitive information to ensure the security of the data; making the functionality of the kernel cryptographic transformations in a separate plug-in library in order to make the study of the decompiled source code on the subject of these reforms meaningless.

Key words: security of applications, mobile devices, data protection, analysis, vulnerabilities.