7. *Metodicheskiy dokument FSTEK Rossii "Metodika opredeleniya ugroz bezopasnosti informatsii v informatsionnykh sistemakh" (proekt)* [Guidance document of the FSTEC of Russia "Methodology for identifying threats to information security in information systems" (project)], 2015. 43 p. Available at: http://fstec.ru/component/attachments/download/812 (accessed 18.09.2019).

8. *Postanovlenie Pravitelstva RF ot 08.02.2018 № 127 "Ob utverzhdenii Pravil kategorirovaniya obektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii, a takzhe perechnya pokazateley kriteriev znachimosti obektov kriticheskoj informatsionnoy infrastruktury Rossiyskoy Federatsii i ikh znacheniy"* [Decree of the Government of the Russian Federation dated February 8, 2018 no. 127 "On Approval of the Rules for the Categorization of Objects of Critical Information Infrastructure of the Russian Federation, as well as a list of indicators of criteria of significance of objects of critical information infrastructure of the Russian Federation and their values"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_290595 (accessed 16.09.2019).

9. *Prikaz FSTEK Rossii ot 25.12.2017 № 239 "Ob utverzhdenii Trebovaniy po obespecheniyu bezopasnosti znachimykh obektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii"* [Order of the FSTEC of Russia dated December 25, 2017 no. 239 "On approving the Requirements to ensure the security of significant objects of the critical information infrastructure of the Russian Federation"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_294287 (accessed 17.09.2019).

10. *Federalnyy zakon ot 26.07.2017 № 187-FZ "O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii"* [Federal Law dated 26.07.2017 no. 187-FZ "On the Security of the Critical Information Infrastructure of the Russian Federation"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_220885 (accessed 15.09.2019).

11. Chernidin Yu. *Sotsialnaya inzheneriya. Vvodnyy material* [Social Engineering. Introductory material]. Available at: https://www.volgablob.ru/blog/?p=1722 (accessed 10.09.2019).

12. *Methodologies for the identification of Critical Information Infrastructure assets and services*. Available at: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis (accessed 10.09.2019).

DOI 10.21672/2074-1707.2019.48.4.135-143
УДК 004.056

КЛАССИФИКАЦИЯ МЕССЕНДЖЕРОВ НА ОСНОВЕ АНАЛИЗА УРОВНЯ БЕЗОПАСНОСТИ ХРАНИМЫХ ДАННЫХ

Статья поступила в редакцию 13.11.2019, в окончательном варианте – 22.11.2019.

Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, e-mail: putyato.m@gmail.com
Макарян Александр Самвелович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, e-mail: msanya@yandex.ru

В статье представлен анализ и классификация мессенджеров на основе анализа уровня безопасности хранимых данных. Произведен обзор современного состояния рынка мобильного приложения класса IM и введены критерии оценки безопасности систем мгновенного обмена сообщениями на основе фактической реализации заявленных алгоритмов и методов шифрования. Рассмотрены аспекты в области безопасности, защиты и хранения данных мессенджеров: данные пользователя на устройстве, журналы событий, ключи шифрования, критичная информация в базах данных, защищенность мессенджеров от атак с физическим доступом к устройству. Производится изучение механизма мессенджера Signal: организация хранения данных и реализация принципов защищенности для хранимых данных. На его примере рассмотрены схемы реализации и использования баз данных мобильного устройства. Выявлены недостатки использования подсистем шифрования и организации баз данных телефонных номеров, отметок регистрации пользователей, текстовых сообщений и медиафайлов, в связи с чем появляется возможность автоматизированного съема критичной информации. В результате сформулированы рекомендации по обеспечению безопасности мессенджеров для разработчиков и пользователей: шифровать вложения мессенджера, переместить все данные из доступного для пользователя пространства памяти в закрытое хранилище приложения, использовать запутывающие названия файлов, шифровать критичные данные в базах данных (сообщения, путь к вложениям, информация о контактах и пр.), использовать дополнительный слой для шифрования критичных данных при условии включенной надстройки, обеспечивающей обязательность ввода парольной фразы для открытия приложения на смартфоне, шифровать непосредственно сами базы данных.

Ключевые слова: анализ, кибербезопасность, форензика, мессенджер, протокол шифрования, защита информации, база данных

Графическая аннотация (Graphical annotation)

CLASSIFICATION OF MESSENGERS BASED ON ANALYSIS OF THE SECURITY LEVEL OF STORED DATA

The article was received by the editorial board on 13.11.2019, in the final version –22.11.2019.

Putyato Michael M., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci (Engineering), Associate Professor, e-mail: putyato.m@gmail.com
Makaryan Alexander S., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci (Engineering), Associate Professor, e-mail: msanya@yandex.ru

The article presents the analysis and classification of instant messengers based on the analysis of the level of security of stored data. A review of the current state of the market for mobile applications of the IM class is carried out and criteria for assessing the security of instant messaging systems based on the actual implementation of the claimed encryption algorithms and methods are introduced. Aspects in the field of security, protection and storage of messenger data are considered: user data on the device, event logs, encryption keys, critical information in the databases, the security of instant messengers from attacks with physical access to the device. The Signal messenger mechanism is being studied: organizing data storage and implementing security principles for stored data. On his example, schemes for the implementation and use of databases of a mobile device are considered. Disadvantages of using the encryption subsystems and organizing databases of telephone numbers, user registration marks, text messages and media files have been identified. In this connection, it becomes possible to automatically extract critical information. As a result, recommendations for securing messengers for developers and users were formulated: encrypt messenger attachments, move all data from the user's available memory space to the application's private storage, use confusing file names, encrypt critical data in databases (messages, attachment path, information about contacts, etc.), use an additional layer of encryption critical for data, provided that an add-in is provided that makes it mandatory enter a passphrase to open the application on your smartphone, directly encrypt the databases themselves.
Key words: analysis, cybersecurity, forensics, messenger, encryption protocol, information security, database

Введение. При рассмотрении современных средств организации электронного общения в первую очередь необходимо отметить системы мгновенного обмена сообщениями (Instant Messaging, IM). Система мгновенного обмена сообщениями – это службы для обмена сообщения-

ми в режиме реального времени. Если раньше основными платформами для реализации общения при помощи электронных средств выступали стационарные и мобильные компьютеры, то сегодня это в основном мобильные устройства связи. В связи с этим на современном рынке мобильных мессенджеров представлено достаточно много мобильных приложений, которые решают одну или несколько следующих задач: передача текста, изображений, видео, звука, в том числе звуковых и видеосообщений, организация видеочата, групповых бесед, конференций и т.д.

Функциональность и актуальные механизмы защиты мобильных мессенджеров. Традиционными функциями программных клиентов для мгновенного обмена сообщениями являются:

- чат (текстовый, голосовой и видеочат);
- передача файлов;
- инструменты для совместной работы в режиме реального времени;
- напоминания и оповещения;
- звонки на компьютер;
- возможность отправки SMS;
- хранение истории общения с контактами;
- индикация сетевого статуса присутствия собеседников (в сети или отсутствует), занесенных в список контактов.

Также использование такой категории программ имеет целый ряд преимуществ:

- экономия времени;
- экономия средств (передача данных использует канал интернет);
- возможность общения в любой ситуации, пользуясь многообразием отправки сообщений (текст, аудио, видео, изображения);
- кроссплатформенность: приложение на смартфоне, веб-версия с использованием браузера, десктопные версии приложений;
- отсутствие понятий роуминга, региональной связи, территориальных ограничений;
- история общения и т.д.

Основываясь на анализе, представленном в статье “Самые защищенные мессенджеры” [4], можно говорить о том, что все современные мессенджеры, такие как Telegram, Signal, Viber, WhatsApp, Briar, ТамТам, ВКонтакте, Facebook Messenger, Wire, Jabber, Riot Matrix, Status, Threema, так или иначе удовлетворяют современным требованиям к безопасности общения и обмена информацией.

В то же время, согласно рейтингу [3], составленному Роскачеством, можем опираться на следующие данные:

- 39 % россиян звонят с помощью мессенджеров чаще или не реже, чем по телефону,
- мессенджеры в 2018 г. занимают первое место по использованию, второе – звонки;
- наиболее популярные мессенджеры: WhatsApp (69 %), Viber (57 %), Skype (45 %);
- в российском сегменте магазинов App Store и Google Play – 49 приложений (25 для iOS и 24 для Android), позволяющих пользователям мгновенно обмениваться сообщениями, в том числе – осуществлять звонки;
- количество приложений, которые перешагнули итоговую отметку в 4 балла, составляет 14 из 49;
- небезопасных приложений выявлено не было, однако у ряда мессенджеров отсутствует сквозное шифрование, что не дает права назвать их защищенными;
- наиболее функциональные: для iOS и Android – «ТамТам» (4,51), ICQ (4,38) и «Mail.ru Агент» (4,38);
- наиболее функциональные: для iOS и Android – «ТамТам» (4,51), ICQ (4,38) и «Mail.ru Агент» (4,38);
- наиболее удобные: для iOS – Messenger (Facebook) (4,85), Threema (4,85) и Skype (4,7); для Android – Threema (4,79), «ВКонтакте» (4,68) и Skype (4,64);
- наиболее удобные: для iOS – Messenger (Facebook) (4,85), Threema (4,85) и Skype (4,7); для Android – Threema (4,79), «ВКонтакте» (4,68) и Skype (4,64);
- наиболее защищенные: для iOS – Wickr Me (4,73), Viber (4,57), WhatsApp (4,40) и Wire (4,31); для Android – Wickr Me (4,73), Viber (4,57), Threema (4,57) и Signal (4,35);
- лучшими по совокупности всех критериев признаны приложения WhatsApp, Viber и Skype для iOS и WhatsApp, Viber и Threema для Android.

И в первом, и во втором представленных обзорах [3, 4] речь в основном идет о механизмах защиты приема и передачи информации, а также о программной реализации и поддержки основных механизмов защиты этих данных.

Глава компании «Интернет-розыск | CABIS» Игорь Бедеров согласен, что все методы шифрования выглядят, по меньшей мере, наивными в то время, когда на рынке имеется возможность «пробить» любой телефонный номер по базе сотового оператора, подделать паспорт и заказать дубль сим-карты в салоне сотовой связи. «На всю операцию будет затрачено не более 30 тыс. рублей. Получив копию сим-карты жертвы, злоумышленник запросто переключит на себя все мессенджеры, социальные сети и электронную почту жертвы», – отмечает господин Бедеров [1].

Ни в одном из этих обзоров, так же как и во многих подобных, не рассматриваются следующие аспекты в области безопасности и защиты данных мессенджеров:

- безопасность хранения данных пользователя на устройстве;
- безопасность журналов событий;
- безопасность хранения ключей шифрования;
- безопасность критичной информации в базах данных мессенджеров;
- защищенность мессенджеров от атак с физическим доступом к устройству.

Исходя из этого, ниже рассмотрим систему критериев, которая позволит объективно оценить безопасность реализации и функционирования локальных механизмов обеспечения работы мобильных приложений, так как при наличии физического доступа к устройству качество реализации именно этой части программ будет отвечать за эффективность обеспечения безопасности данных в целом.

Есть мессенджеры, которые вообще не хранят историю переписки на сервере. В этом случае устройство (ваш телефон, например) является одновременно и клиентом, и сервером. Это самый безопасный способ, но мессенджеры «без истории» не пользуются популярностью. Одна из причин – мультиплатформенность мессенджеров с «облачной памятью»: пользователь может войти в свой аккаунт одновременно на телефоне, планшете и компьютере [5].

Анализ использования механизмов защиты в мессенджерах. Для нашего анализа мы выбрали мессенджеры, которые занимают лидирующие позиции на рынке приложений систем мгновенного обмена сообщениями.

Для сравнения программных средств мы сформулировали и уточнили критерии, которые позволяют произвести оценку механизмов защиты с учетом специфики хранения и обработки приложениями критичных данных. Исходя из принципа комплексности, критерии объединены в группы влияния на безопасность мобильного приложения при использовании.

1. Локальные критичные данные – 50 %:

1a. Информация профиля (Не хранится; Хранится, шифруется на стороне клиента; Хранится, не шифруется на стороне клиента).

1b. Метаданные чата (Не хранится; Хранится).

1c. Список контактов (Не хранится; Хранится).

1d. E2EE[6] Cloud Backup (Имеется; Не имеется).

2. Сетевые критичные данные – 20 %:

2a. Подтверждение контракта (Имеется; Не имеется).

2b. Шифрование группового чата (Имеется; Не имеется).

2c. Шифрование передачи файлов (Имеется; Не имеется).

2d. Открытый ключ и IP не связаны (Имеется; Не имеется).

2e. Асинхронное шифрование беседы (Имеется; Не имеется).

2f. Зашифрованные данные клиента (Имеется; Не имеется).

2g. Самоуничтожающиеся сообщения (Имеется; Не имеется).

3. Шифрование [2] – 30 %:

3a. Шифрование (Симметричное) (Имеется; Не имеется).

3b. Шифрование (Ассиметричное) (ECC 256; RSA 2048; Нет).

3c. Forward secrecy (Имеется; Не имеется).

3d. Многократное шифрование (Имеется; Не имеется).

Произведем оценку характеристик систем мгновенного обмена сообщениями, используя описанные выше формальные критерии. Результаты анализа представлены в таблице.

Таблица – Сравнение характеристик систем мгновенного обмена сообщениями

№ п/п	Наименование критерия	Telegram	Signal	WhatsApp	Threema	Viber
1a	Информация профиля	0,0	0,5	0,0	0,5	0,0
1b	Метаданные чата	0,5	0,5	0,0	0,5	0,0
1c	Списки контактов	0,0	0,5	0,0	0,5	0,0
1d	E2EE Cloud Backup	0,0	0,0	0,5	0,5	0,0
2a	Подтверждение контракта	0,2	0,2	0,2	0,2	0,2
2b	Шифрование группового чата	0,0	0,2	0,2	0,2	0,0
2c	Шифрование передачи файлов	0,2	0,2	0,2	0,2	0,2
2d	Открытый ключ и IP не связаны	0,0	0,2	0,2	0,2	0,2
2e	Асинхронное шифрование беседы	0,0	0,2	0,2	0,2	0,2
2f	Зашифрованные данные клиента	0,2	0,2	0,2	0,2	0,2
2g	Самоуничтожающиеся сообщения	0,2	0,2	0,0	0,0	0,0
3a	Шифрование: Симметричное	0,3	0,3	0,3	0,3	0,3
3b	Шифрование: Ассимметричное	0,3	0,6	0,6	0,6	0,6
3c	Forward secrecy	0,3	0,3	0,3	0,0	0,3
3d	Многократное шифрование	0,3	0,3	0,3	0,3	0,3
Итог		2.5	4,4	3,2	4,4	2,5

Анализ использования механизмов обеспечения безопасности в мессенджерах показывает, что из рассмотренных вариантов лучшие результаты с точки зрения безопасности хранимых данных показывают приложения Signal [7] и Threema [8].

Реализация механизмов защиты мессенджера Signal. Рассмотрим детальнее соответствие заявленных характеристик действительному положению дел на примере мессенджера Signal.

В папке с базами данных мессенджера имеются 3 файла:

- “canonical_address.db”;
- “messages.db”;
- “whisper_directory.db”.

Все базы не зашифрованы и доступны для открытия при наличии физического доступа к смартфону. Если исследовать таблицы, то можно получить следующие результаты.

1. База данных canonical_address.db содержит в себе минимальное количество информации: номера телефонов и их соответствие некоторому идентификатору (рис. 1).

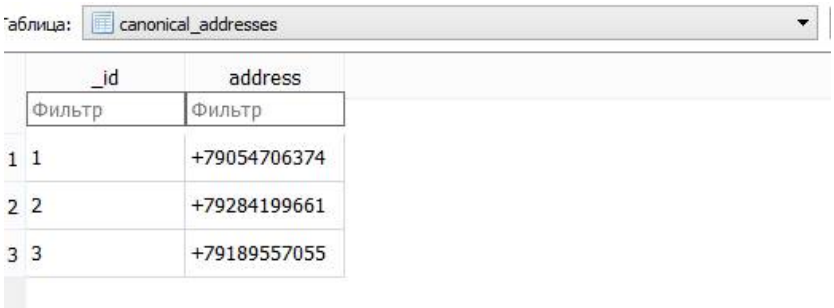

Рисунок 1 – Фрагмент базы данных canonical_address.db

2. При исследовании базы данных whisper_directory.db ситуация повторяется: имеется таблица, в которой содержатся все считанные номера из устройства с дополнительной отметкой о том, какие из них зарегистрированы в Signal (рис. 2). Если провести параллель с первой базой данных и сопоставить номера, то можно сделать вывод о том, что в первой базе содержатся зарегистрированные в системе Signal аккаунты с соответствующими им номерами.

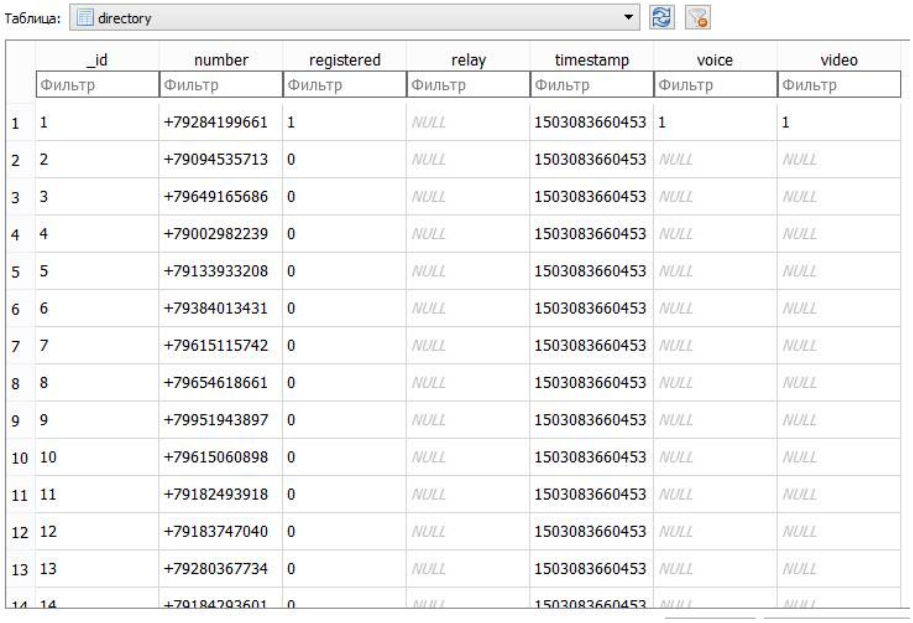
Таблица: directory

	_id	number	registered	relay	timestamp	voice	video
	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр
1	1	+79284199661	1	NULL	1503083660453	1	1
2	2	+79094535713	0	NULL	1503083660453	NULL	NULL
3	3	+79649165686	0	NULL	1503083660453	NULL	NULL
4	4	+79002982239	0	NULL	1503083660453	NULL	NULL
5	5	+79133933208	0	NULL	1503083660453	NULL	NULL
6	6	+79384013431	0	NULL	1503083660453	NULL	NULL
7	7	+79615115742	0	NULL	1503083660453	NULL	NULL
8	8	+79654618661	0	NULL	1503083660453	NULL	NULL
9	9	+79951943897	0	NULL	1503083660453	NULL	NULL
10	10	+79615060898	0	NULL	1503083660453	NULL	NULL
11	11	+79182493918	0	NULL	1503083660453	NULL	NULL
12	12	+79183747040	0	NULL	1503083660453	NULL	NULL
13	13	+79280367734	0	NULL	1503083660453	NULL	NULL
14	14	+79184293601	0	NULL	1503083660453	NULL	NULL

Рисунок 2 – Фрагмент базы данных whisper_directory.db

3. Исследование базы messages.db (рис. 3) показало, что структура таблиц очень похожа на структуру, которая используется в стандартном Android-приложении для приема и отправки SMS- и MMS-сообщений.

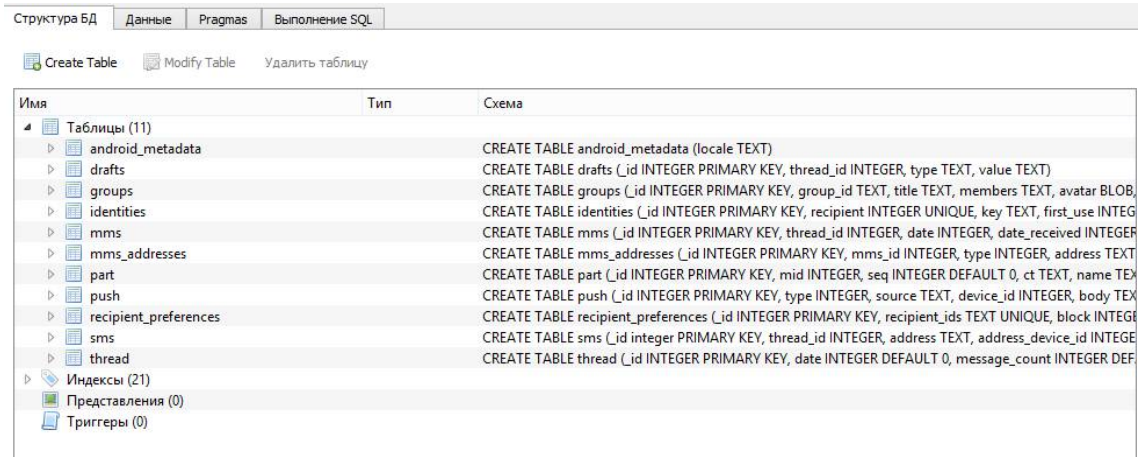

Рисунок 3 – Фрагмент базы данных messages.db

Нас интересуют следующие таблицы:

- “sms”, содержащая информацию о текстовых сообщениях;
- “mms”, содержащая информацию о медиасообщениях;
- “thread”, содержащая информацию об активных чатах;
- “part”, содержащая сведения о файлах медиасообщений.

Таблицы “sms” и “mms” имеют сходную структуру, так что рассмотрим только одну таблицу – “sms” (рис. 4).

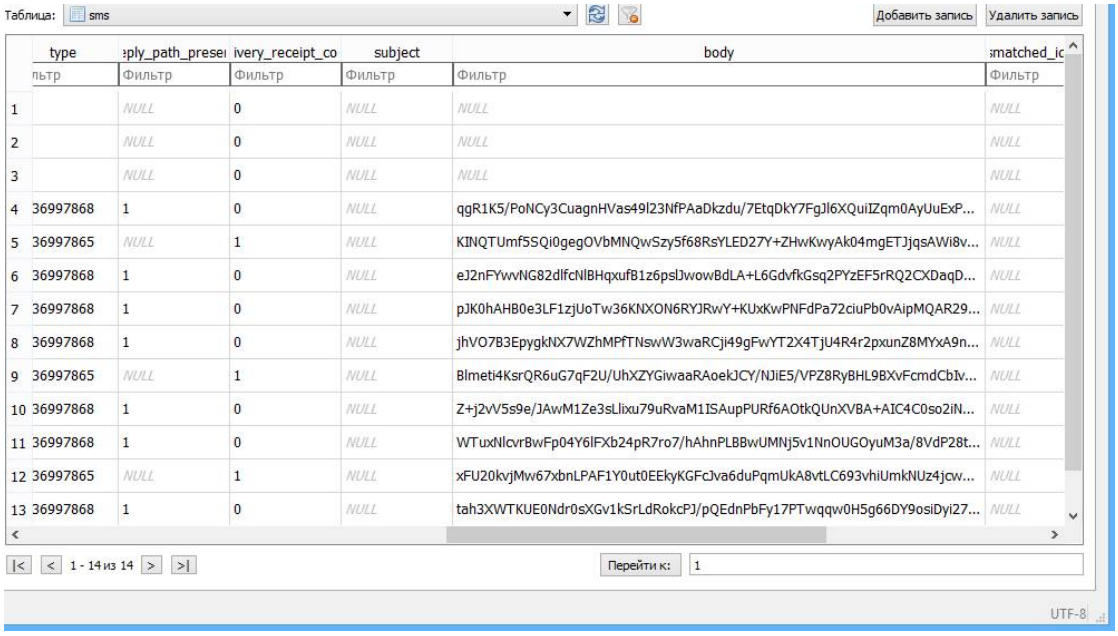

Рисунок 4 – Фрагмент, показывающий структуру таблицы sms

Рассматривая проблему читаемости таблицы, мы заметили, что все сообщения имеют примерно одинаковую структуру (рис. 5) построения (последовательность “=” является завершением потока). Возможно, есть некий алгоритм, для работы которого это важно.

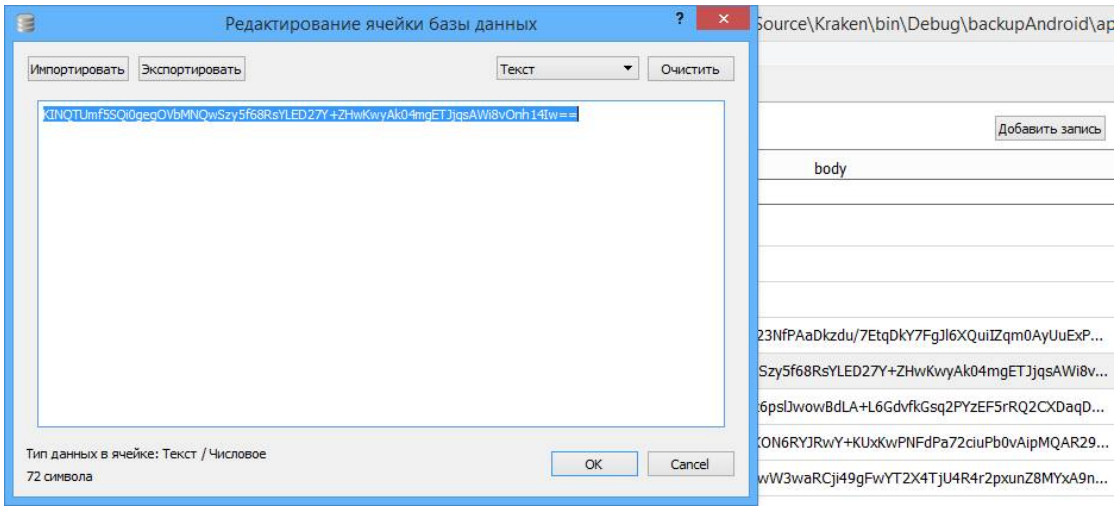

Рисунок 5 – Пример структуры сообщения в таблице sms

Исследование показывает следующее:

1. Базы данных мессенджеров в мобильных устройствах не зашифрованы, так что возможно составить запросы для автоматизированного съема критичной информации, что дает возможность получения несанкционированного доступа к данным пользователя устройства.
2. Есть взаимосвязь между номером телефона и идентификатором учетной записи Signal, однако данных о закрепленных за номерами персональных данных найдено не было.
3. Были найдены зашифрованные файлы вложений.
4. Содержание сообщений передаваемых пользователями зашифровано и (или) закодировано.

Чтобы извлечь информацию о сообщениях, необходимо составить следующий запрос для базы данных “messages.db” с использованием языка программирования SQL: “Select address, datetime(date/1000,'unixepoch'), type, body from sms order by date”.

Для получения информации о вложениях запрос для базы данных “messages.db” с использованием языка программирования SQL выглядит следующим образом: “Select recipient_ids, datetime(mms.date/1000,'unixepoch'), msg_box, body, ct, _data from mms left join part on mid = mms.id left join thread on thread_id = thread.id order by mms.date”.

Чтобы получить информацию о телефонных номерах пользователя устройства, необходимо воспользоваться следующим скриптом для базы данных “canonical_address.db” с использованием языка программирования SQL:“Select_id, address from canonical_addresses”.

Выводы. В погоне за выгодой и привлечением новых пользователей компании разработчики мессенджеров идут на хитрости, связанные с реализацией безопасности своих приложений; декларируют механизмы защиты, которые так или иначе заставляют пользователей чувствовать себя защищенными. Однако на самом деле все далеко не так.

На примере одного из «безопасных» мессенджеров мы продемонстрировали, что системы реализованы с нарушением целостности системы защиты данных. Функционирование механизмов происходит на открытых, доступных, программных инфраструктурах мобильных устройств: БД, средства передачи, журналы событий и т.д. В связи с этим дадим некоторые рекомендации по обеспечению безопасности мессенджеров для разработчиков:

- шифровать вложения мессенджера;
- переместить все данные из доступного для пользователя пространства памяти в закрытое хранилище приложения;
- использовать запутывающие названия файлов;
- шифровать критичные данные в базах данных (сообщения, путь к вложениям, информация о контактах и пр.);
- использовать дополнительный слой для шифрования критичных данных при условии включенной надстройки необходимости ввода парольной фразы при открытии приложения на смартфоне;
- шифровать непосредственно сами базы данных.

В дальнейших исследованиях мы вернемся к более подробному анализу каждого из представленных в сравнении мессенджеров, а также продолжим анализ механизмов и их реализаций на практике.

Библиографический список

1. Безопасность до блокировки доведет // Коммерсантъ. – Режим доступа: https://www.kommersant.ru/doc/3379658, свободный. – Заглавие с экрана. – Яз. рус.

2. Жданов О. Н. Методы и средства криптографической защиты информации / О. Н. Жданов, В. В. Золотарев. – Красноярск : Редакционно-издательский отдел СибГАУ, 2007. – 253 с.

3. Мессенджеры // Роскачество портал для умного покупателя. – Режим доступа: https://rskrf.ru/ratings/tekhnologii/mobilnye-prilozheniya/mp-quot-messendzhery-quot, свободный. – Заглавие с экрана. – Яз. рус.

4. Самые защищенные мессенджеры // Spy-soft.net информационная безопасность на практике. – Режим доступа: http://www.spy-soft.net/most-secure-messengers/, свободный. – Заглавие с экрана. – Яз. рус.

5. Они читают ваши сообщения: как найти безопасный мессенджер // Internet UA. – Режим доступа: http://internetua.com/oni-csitauat-vashi-soobsxeniya-kak-naiti-bezopasnyi-messendjer, свободный. – Заглавие с экрана. – Яз. рус.

6. A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work? // SSD.EFF.ORG. – Режим доступа: https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work, свободный. – Заглавие с экрана. – Яз. англ.

7. Technical Information // Signal. – Режим доступа: https://signal.org/docs/, свободный. – Заглавие с экрана. – Яз. англ.

8. Threema Gateway // Threema.Gateway. – Режим доступа: https://gateway.threema.ch/en, свободный. – Заглавие с экрана. – Яз. англ.

References

1. Bezopasnost do blokirovki dovedet [Security will bring to blocking]. *Kommersant* [Businessman]. Available at: https://www.kommersant.ru/doc/3379658.

2. Zhdanov O. N., Zolotarev V. V. *Metody i sredstva kriptograficheskoy zashchity informatsii* [Methods and means of cryptographic information protection]. Krasnoyarsk, Editorial and Publishing Department of SibSAU, 2007.

3. Messendzhery [Messengers]. *Roskachestvo portal dlya umnogo pokupatelya* [Roskachestvo portal for a smart buyer]. Available at: https://rskrf.ru/ratings/tekhnologii/mobilnye-prilozheniya/mp-quot-messendzhery-quot.

4. Samye zashchishchennye messendzhery [The most secure messengers]. *Spy-soft.net informatsionnaya bezopasnost na praktike* [Spy-soft.net information security in practice]. Available at: http://www.spy-soft.net/most-secure-messengers/.

5. Oni chitayut vashi soobshcheniya: kak nayti bezopasnyy messendzher [They read your messages: how to find a secure messenger]. *Internet UA*. Available at: http://internetua.com/oni-csitauat-vashi-soobsxeniya-kak-naiti-bezopasnyi-messendjer.

6. A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work? *SSD.EFF.ORG*. Available at: https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work.

7. Technical Information. *Signal.* Available at: https://signal.org/docs/.

8. Threema Gateway. *Threema.Gateway.* Available at: https://gateway.threema.ch/en.