УДК 004

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ

Г. А. Положий, А. Р. Тосунова, О. А. Сафарьян, Л. В. Черкесова
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

В статье рассмотрены популярные на сегодняшний день системы мгновенного обмена сообщениями — мессенджеры. Проведен сравнительный анализа по функционалу манипуляций с сообщениями, кроссплатформенности, возможности групповых чатов и звонков. Представлен обзор применяемых протоколов шифрования в различных системах.
Ключевые слова: мессенджер, протокол шифрования, сквозное шифрование, шифрование Вернама, Python, Signal.

COMPARATIVE ANALYSIS OF INSTANT MESSAGING SYSTEMS

G. A. Polozhiy, A. R. Tosunova, O. A. Safaryan, L. V. Cherkesova
Don State Technical University (Rostov-on-Don, Russian Federation)

The article discusses the current popular instant messaging systems. The paper provides a comparative analysis of the functionality of manipulations with messages, a cross-platform property and capabilities of group chats and calls. It also has an overview of the encryption protocols used in various systems
Keywords: messenger, encryption protocol, end-to-end encryption, Vernam encryption, Python, Signal.

Введение. После появления интернета и его всеобщей глобализации, а также распространения доступных, но при этом достаточно мощных мобильных устройств, приложения мгновенного обмена сообщениями прочно вошли в повседневную жизнь. Почти у каждого обладателя смартфона среди множества приложений можно найти один из популярнейших мессенджеров.

Современные мессенджеры обеспечили новую свободу общения, став более гибкой, доступной и качественной альтернативой как наземной, так и сотовой связи. С ростом популярности мобильных устройств мессенджеры трансформировались и распространились, и это привело к обострению конкуренции в сегменте. Постоянная конкуренция, в свою очередь, мотивирует гигантов этого рынка к постоянному совершенствованию и улучшению своих продуктов, так что обновления приложений выходят регулярно и несут в себе, порой, значимые изменения. Поэтому любая оценка характеристик и сравнительный анализ может потерять свою актуальность с выходом очередного обновления.

Цель работы — это проведение сравнительного анализа систем мгновенного обмена сообщениями для определения баланса между удобством пользовательского интерфейса и безопасностью общения. Эта работа является способом внесения своего вклада в развитие информационной среды современного общества.

Цель определила следующие задачи:

- рассмотреть популярные системы мгновенного обмена сообщениями;
- провести сравнительный анализ характеристик этих систем.

На сегодняшний день существование человечества невозможно без виртуальных средств общения. Это высоко конкурентная среда.

Обзор популярных на сегодняшний день мессенджеров

Мессенджер — это программное средство, мобильное приложение или веб-сервис для обмена сообщениями в реальном времени через интернет.

Зачастую, мессенджеры работают не самостоятельно, а подключаются к какому-либо компьютеру, который является центральным в сети обмена сообщениями, он называется сервером. Именно поэтому мессенджеры называются «клиентами».

Для широкого круга пользователей известно определенное количество популярных систем обмена сообщениями, таких как WhatsApp, Viber, Messenger from Facebook, Telegram, Skype. Все сети были разработаны разными группами разработчиков, они используют разные протоколы и серверы, имеют различия в своих условиях и особенностях. Различные сети не имеют прямой связи между собой. Это значит, что пользователь Skype не может отправить сообщение пользователю What's App, но любой пользователь может состоять в нескольких сетях.

Запущенный в 2009 году What's App стал первым популярным мессенджером, предназначенным именно для смартфонов с привязкой к номеру телефона пользователя, в дальнейшем породившим множество копий и вариаций — LINE, Wazapp, Viber, Snapchat, Telegram и т.п.

А самые популярные мессенджеры на сегодняшний день — WhatsApp, Viber, Messenger from Facebook, Telegram, Skype; все перечисленные мессенджеры обладают VoIP**.** Voice over Internet Protocol или IP-телефония — это голосовая связь через интернет (в отличии от традиционной телефонной связи, которая осуществляется через телефонные линии или мобильную сеть).

Рассмотрим рейтинг, представленный компанией Brand Analitics. Сообщается, что для расчета рейтинга проанализированы 2,1 млрд русскоязычных сообщений социальных медиа за август 2019 года. Поток включает социальные сети ВКонтакте, Одноклассники, Twitter, Facebook, Instagram, YouTube, Мой Мир, МирТесен, а также блоги, форумы, публичные каналы мессенджеров, комментарии к новостным статьям. Сообщения от ботов не включены в анализ.

Из статистики компании Brand Analitics становится очевидным лидерство тройки основных конкурирующих систем: WhatsApp, Viber, Telegram [1].

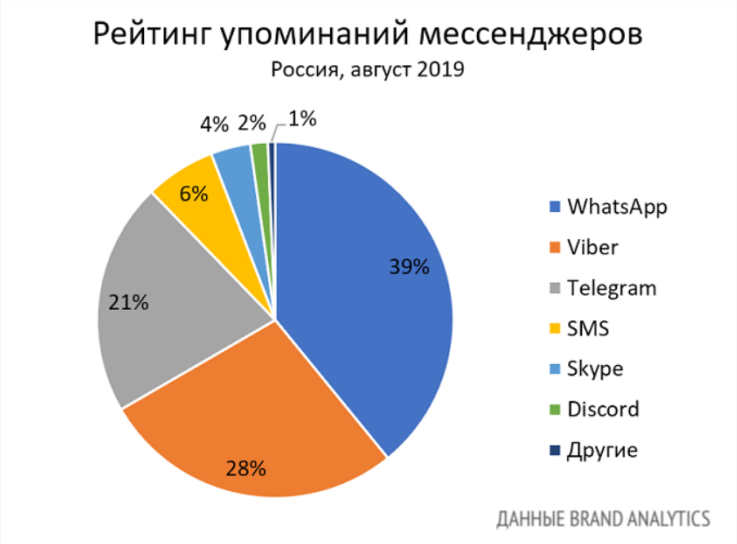

Рис. 1. Рейтинг популярности мессенджеров

Практичнее будет рассматривать три основных лидера рынка для проведения сравнительного анализа.

Основная часть

Для каждого приложения можно выделить недостатки в манипуляциях с сообщениями и файлами в сравнении с другими мессенджерами. Для WhatsApp: ограниченная поддержка форматирования текста, ограничение на объем видео или медиа-файлов, отсутствует поддержка ботов и опросов, нет возможности ускорения аудиосообщений, а функция удаления сообщений реализована только с уведомлением об удалении. Для Viber: полное отсутствие форматирования текста, потеря качества передаваемого изображения, нет возможности ускорения аудиосообщений и удаление сообщений только с уведомлением об удалении. Для Telegram: нет таких ограничений, как у других приложений.

Сравнение характеристик систем мгновенного обмена сообщениями

WhatsApp обладает браузерной версией, которая синхронизируется через считанный QR-код, поэтому без наличия мобильного приложения нет возможности воспользоваться веб-версией. Контакты синхронизируются автоматически. В приложении можно писать сообщения, а звонки недоступны. История сообщений не подтягивается. У Telegram тоже есть веб-версия, и это самый дружественный мессенджер. Везде имеет схожий интерфейс, а все сообщения отображаются абсолютно на всех устройствах, потому что хранятся на серверах. Viber существует для всех платформ. Его можно поставить и на ПК, и на смартфон, но веб-версии нет.

Групповые чаты. Поддерживают все мессенджеры. Отличия состоят только в количестве аудитории. Telegram — 100 000, WhatsApp — максимум 256 пользователей. В хвосте оказался Viber — 250 человек, но при этом есть возможность добавления контактов в несколько чатов одновременно.

Голосовые звонки. Поддерживаются всеми приложениями, но Viber поддерживает звонки как внутри приложения, так и на телефонные номера — ViberOut, что является уникальной функцией, отличающей эту систему от остальных.

Видео звонки: присутствуют в Viber и WhatsApp, видео конференции — только WhatsApp. В Telegram функция частично реализована в виде видео сообщений, они записываются аналогично аудио сообщениям.

При этом Telegram имеет больше надстроек конфиденциальности, как пример, параметр видимости номера телефона может принимать значения: «всем, вашим контактам, никому».

В свою очередь, в WhatsApp реализованы такие уникальные функции, как создание персонализированного статуса, просмотр статусов контактов, формирование ответов и пересылки.

Все мессенджеры имеют свои недостатки, но также у них есть и достоинства, присущие только им. Процесс доработки и поддержки эксплуатации непрерывен, так что каждый день могут выходить обновления с новыми исправлениями.

Рассмотрим протоколы шифрования

В отличие от WhatsApp и Viber, Telegram использует для шифрования собственную симметричную схему шифрования под названием MTProto. Протокол был разработан Николаем Дуровым и другими разработчиками в Telegram и основан на 256-битном симметричном шифровании AES, 2048-битном шифровании RSA и обмене ключами Диффи-Хеллмана [2].

Сквозное шифрование, или end-to-end encryption (E2EE), считается наиболее эффективным решением проблемы безопасности от попыток злоумышленников ознакомиться с онлайн перепиской. Смысл E2EE в общем случае заключается в том, что ключи хранятся только на устройствах собеседников и не попадают на сервер, но это только общее описание, не отражающее всего происходящего при использовании алгоритма.

С 2016 года и обновлением версии 2.16.12 WhatsApp применил сквозное шифрование (end-to-end) для всех пользователей на базе разработок Signal (Open Whisper Systems). Предоставляемое Signal

сквозное шифрование сегодня применяется во многих мессенджерах: WhatsApp, Facebook Messenger, Viber, Google Allo, G Data Secure Chat. Они все используют оригинальную или немного модифицированную версию Signal Protocol, порой меняя названия. Например, у Viber это протокол Proteus — фактически, тот же Signal только с другими криптографическими особенностями [3].

Но, хотя реализации сквозного шифрования является весьма схожей, само приложение также может скомпрометировать личные данные иными способами. Так, в Viber и WhatsApp есть функция создания резервной копии истории переписки. При этом, защита у облачной и локальной копии переписки не является стойкой, а метаданные не имеют никакой криптозащиты — эта информация оглашена в лицензионном соглашении.

Но E2EE имеет особенности для каждого мессенджера. В WhatsApp шифрование такое же, как в Signal, за исключением того, что смена основного ключа абонента WhatsApp не останавливает отправку ему сообщений, что является большой уязвимостью. В Viber сквозное шифрование является неактивным по умолчанию. В Telegram E2EE также используется, но применяется только в секретных чатах.

В отличие от рассмотренных мессенджеров, большим достоинством разработанной системы мгновенного обмена сообщениями является использование не стандартного протокола шифрования, а схемы, сочетающей в себе алгоритмы шифрования Вернама и RSA [4].

При передаче сообщения (или истории сообщений) от сервера к клиенту или от клиента к серверу данные шифруются симметричным алгоритмом Вернама, что обеспечивает абсолютную стойкость против попыток взлома. А симметричный ключ шифруется асимметричным алгоритмом RSA. Ключи RSA, как клиента, так и сервера, имеют битовую длину не менее 3072 бит, что позволяет обеспечить эффективную защиту ключа Вернама. Во всех применяемых методах случайные числа генерируются криптостойкими, что сводит к минимуму вероятность злоумышленника подобрать данные числа. При всем этом скорость обмена сообщений сохраняется на высоком уровне [4].

Представим данные методы, реализованные на языке Python, используемые на стороне сервера для шифрования и расшифрования данных сообщения. Данный алгоритм осуществляет шифрование методом Вернама, где генерация гаммы использует криптостойкие случайные числа.

```
def vernam_encrypt(self, content):
    key = [secure_rand_gen.randrange(150) for i in range(len(content))]
    encrypted_content = []
    for i in range(len(content)):
       encrypted_content.append(ord(content[i])^key[i])
    return {
       'encrypted_content': encrypted_content,
       'key': key
       }
```

Также представлен алгоритм расшифрования сообщения клиента, зашифрованного методом Вернама.

```
def vernam_decrypt(self, cipher_pad, key):
    text = ''
    for i in range(len(cipher_pad)):
       text += chr(cipher_pad[i]^key[i])
    return text
```

Заключение. Почти все наиболее распространенные на территории России мессенджеры имеют различия в функционале, что в некоторых случаях может выгодно отличать рассматриваемый мессенджер. В целом нет кардинальных различий в пользовательском

функционале. Вопрос о безопасности стоит намного острее, потому что каждый мессенджер, несмотря на длительное существование, имеет уязвимость в своей системе безопасности, риск утечки личной переписки, либо фотографий, что является весомым фактом.

Библиографический список

1. Мессенджеры в России 2019 : новые лидеры и перспективные новички [Электронный ресурс] / Википедия. — URL : https://br-analytics.ru/ blog/messengers-in-russia-2019/ (дата обращения : 02.03.2020).

2. Бабаш, А. В. Криптографические методы защиты информации / А. В. Бабаш, Е. К. Баранова. — Москва : КНОРУС, 2016. — 192 с.

3. Протокол Signal [Электронный ресурс] / Википедия. — URL : https://ru.wikipedia.org/wiki/Протокол_Signal (дата обращения : 27.02.2020).

4. Панасенко, С. П. Алгоритмы шифрования / С. П. Панасенко. — Санкт-Петербург : БХВ , 2015. — 576 с.

5. Черемушкин, А. В. Криптографические протоколы. Основные свойства и уязвимости / А. В. Черемушкин. — Москва : Академия, 2009. — 272 с.

Об авторах:

Положий Глеб Андреевич, студент кафедры «Кибербезопасность информационных систем» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), glebpolozhii@mail.ru

Тосунова Анна Ринальдовна, студент кафедры «Кибербезопасность информационных систем» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), annatosunova@mail.ru

Сафарьян Ольга Александровна, доцент кафедры «Кибербезопасность информационных систем» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), кандидат технических наук, доцент, safari_2006@mail.ru

Черкесова Лариса Владимировна, профессор кафедры «Кибербезопасность информационных систем» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), доктор физико-математических наук, профессор, chia2002@inbox.ru

Authors:

Polozhiy, Gleb A., student, Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), glebpolozhii@mail.ru

Tosunova, Anna R., student, Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), annatosunova@mail.ru

Safaryan, Olga A., associate professor, Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), Cand. Sci., Associate professor, safari_2006@mail.ru

Cherkesova, Larisa V., professor, Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), Dr. Sci., Professor, chia2002@inbox.ru