УДК 004.773

О. С. Осинцев[1] *

Исследование протокола мгновенного обмена сообщениями Matrix

[1] Национальный Исследовательский Ядерный Университет «МИФИ», г. Москва, Российская Федерация
* e-mail: osincevoleg@mail.ru

Аннотация. В статье обозреваются протоколы мгновенного обмена сообщениями, рассматриваются возможности зашифрованной передачи сообщений между пользователями, а также возможности аудита безопасности. В ней также рассмотрены протоколы с закрытым и открытым алгоритмами шифрования и определены их преимущества и недостатки. Был исследован современный алгоритм шифрования сообщений и выведены его преимущества в защите передаваемых данных от злоумышленников. В качестве целевого протокола мгновенного обмена сообщениями, основанного на разобранном алгоритме, был выбран *Matrix.* Как аргументы выбора данной технологии приведены уникальные функции и особенности инструмента, показывающие эффективность протокола при создании собственных чатов и мессенджеров. В результате исследования были систематизированы преимущества и недостатки *Matrix*, а также определены дальнейшие направления изучения, включая разработку модулей, улучшающих существующие решения протокола.

Ключевые слова: мгновенный обмен сообщениями, *IM, Matrix, Signal*, клиент-сервер, технология Интернет

O. S. Osincev[1] *

Investigation of the Matrix instant messaging protocol

[1] National Research Nuclear University «Mephi», Moscow, Russian Federation
* e-mail: osincevoleg@mail.ru

Abstract. This article reviews instant messaging protocols, discusses the possibilities of encrypted messaging between users, as well as the possibilities of security auditing. It considers protocols with closed and open encryption algorithms and identifies their advantages and disadvantages. A modern message encryption algorithm was investigated and its advantages in protecting transmitted data from intruders were deduced. *Matrix* was chosen as the target instant messaging protocol based on the parsed algorithm. As arguments for choosing this technology unique functions and features of the tool are given showing the effectiveness of the protocol when creating your own chats and instant messengers. As a result of the study, the advantages and disadvantages of *Matrix* were systematized, and further areas of study were identified, including the development of modules that improve existing protocol solutions.

Keywords: instant messaging, *IM, Matrix, Signal*, client-server, Internet technology

Введение

Конец 20-го века стал бумом развития технологии глобальной вычислительной сети Интернет для всего мира. В дополнении к этому, технология стала доступней и значимей для обычных пользователей чем ранее, когда технология была реализована только для государственной и военной индустрии. Этот про-

гресс развития Интернета повлек за собой создание стандартов, технологий и протоколов взаимодействия между пользователем с использованием глобальной вычислительной сети.

Особое место в развитии Интернета занимает обеспечение безопасности пользователя. При передаче данных по глобальной вычислительной сети с применением протокола *TCP/IP* информация формируется и передается от определенного отправителя и должна достигнуть определенного адресата. При этом, если при передаче данных по сети в недостаточной степени обеспечивалась безопасность, то коммуникация между отправителем и адресатом может быть скомпрометирована и нарушена, вследствие чего будут нарушены следующие характеристики информационной безопасности: конфиденциальность, целостность, доступность, отказоустойчивость [1]. Предотвращение вмешательств злоумышленников в коммуникации между пользователями сети обеспечивается различными протоколами шифрования, методиками защиты от активных и пассивных атак, анализом и тестированием программных реализаций на наличие уязвимостей и возможных угроз системы.

Протоколы мгновенного обмена сообщениями включают в себя комплекс, состоящий из методов шифрования, аутентификации и создания соединений между пользователями внутри глобальной сети. Они являются основой для разработки любых безопасных мессенджеров и чатов, объявляемых в публичных пространствах, а также создаваемых для частных лиц. Без должного внимания к обеспечению информационной безопасности такой подход приведет к несанкционированному доступу к персональным данным пользователей, а также к конфиденциальной информации, передаваемой между пользователями внутри систем мгновенного обмена сообщениями.

Исследование предметной области

К началу 2023 года существуют десятки протоколов, на основе которых реализуется общение между пользователями, а также шифрование пересылаемых сообщений между пользователями внутри сети. Данные технологии лежат в основе современных приложений обмена сообщениями, таких как *WhatsApp, Telegram, VKmessenger, Viber, Skype*. Они реализуют соединение клиентов внутри своих сетей, а также шифруют сообщения для безопасной пересылки сообщений.

Большинство популярных мессенджеров используют собственные разработки и, в основном, реализация данных протоколов является закрытой от пользовательского аудита применяемых алгоритмов и методов. Мессенджеры *Telegram* и *Skype*, являющиеся продуктами крупных компаний и программами с закрытым исходным кодом, могут содержать различные уязвимости. Но из-за ограниченного доступа к реализации программы проводить аудит безопасности приложений возможно только самими разработчиками при заказе услуг проверки или внутренним аудитом [2].

Криптографические протоколы собственной разработки являются достаточно затратным и ненадежным инструментом шифрования. Такой подход к без-

опасности при передаче сообщений зависит от реализации протокола и подробного внутреннего аудита и может предоставлять угрозу системе, в которой используется этот протокол. Этот вопрос подробно рассматриваются в [3, 4]. В результате использование этих протоколов может привести к огромному ущербу, если уязвимость сможет пройти внутренние проверки.

От этого недостатка избавлены протоколы с открытыми алгоритмами шифрования. Данные инструменты открыто лицензируются и предоставляют свое содержимое для всех пользователей, захотевших воспользоваться протоколом. Так, подобный подход реализуется в приложениях *Whatsapp* и *Element*. В данном случае безопасность передаваемых сообщений обеспечивается не закрытыми алгоритмами шифрования, а секретными ключами, при помощи которых шифруются сообщения [5].

Одним из современных протоколов с открытой реализацией для обмена сообщениями между пользователями внутри сети является *Signal*. Данный протокол обеспечивает сквозное шифрование сообщений алгоритмом двойного храповика. Алгоритм сочетает в себе реализации симметричного и ассиметричного шифрования, где ассиметричными ключами генерируется глобальный симметричный ключ, а после из полученного значения создаются новые симметричные ключи, направленные на шифрование сообщений.

Алгоритм работает на стороне клиентов, в которых происходит общение. При помощи ассиметричного шифрования, где генерируется общий секрет из секретного ключа и открытого ключа, и функции *KDF* генерируется общий симметричный ключ *root key* и ключ сессии *session key 1*. При отправке сообщения, функция *KDF* создает два ключа: *session key 2* и *message key 1*. Последним ключом шифруется сообщение, а после таким же ключом расшифровывается на другой стороне. Алгоритм проиллюстрирован на рис. 1.

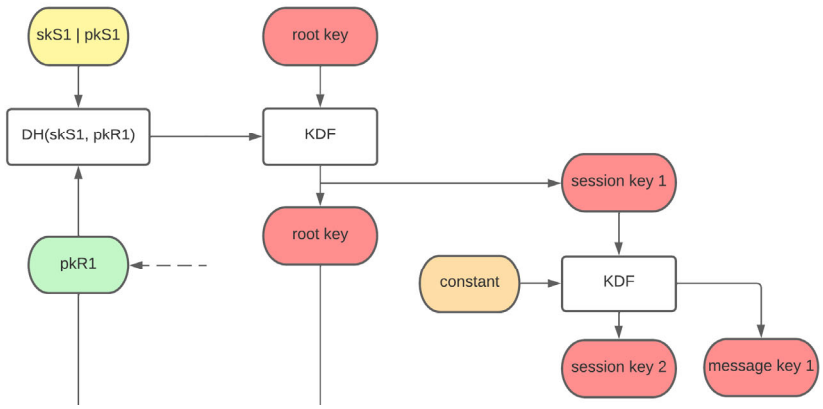

Рис. 1. Алгоритм двойного храповика (отправка сообщения)

Если сообщения отправляет собеседник, который до этого читал сообщения, при помощи ассиметричного шифрования генерируется новый *root key*, и далее функциями генерируются *session key* и *message key* как показано на рис. 2.

Плюсы данного алгоритма заключаются в том, что если злоумышленник получит симметричный ключ шифрования сообщений, то он сможет расшифровать сообщения, которые зашифровывались этим ключом и далее до тех пор, пока собеседник не отправит свое сообщение, чем инициализирует генерацию нового глобального симметричного ключевого значения. Данная технология ограничивает злоумышленника в возможностях следить за переписками между клиентами [6].

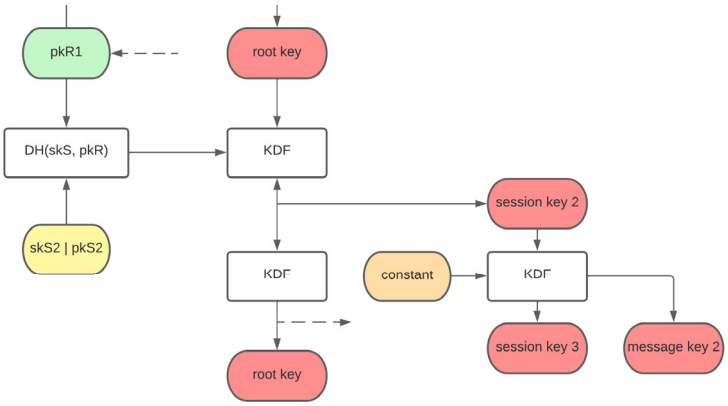

Рис. 2. Алгоритм двойного храповика (принятие сообщения)

На основе данного алгоритма, были реализованы алгоритмы шифрования *Olm* и *Megolm*, являющиеся криптографическими инструментами протокола *Matrix*. *Olm* реализует стандартный двойной храповик и используется для шифрования коммуникации между двумя пользователями. *Megolm* – расширенная версия алгоритма *Olm*, предназначенная для шифрования сообщений между большим количеством клиентов. Данная модификация алгоритма необходима для синхронизации состояний храповика на всех клиентах, находящихся в одном пространстве сети, называемом комнатой [7].

Программная реализация этих алгоритмов является несовершенной, вследствие чего, разработчики протокола *Matrix* улучшают его функционал, развивая и модернизируя библиотеки шифрования. В скором будущем существующую криптографическую библиотеку *Libolm* заменит более совершенная *Vodozemac*. При проведении внутреннего независимого аудита безопасности реализующегося инструмента шифрования Vodozemac, который впоследствии заменит основной инструмент *Libolm* протокола *Matrix*, компания *Least Authority* обнаружила ряд проблем, часть из которых были решены за время проверки, а оставшаяся часть будет рассмотрена во время доработки инструмента. Также во время аудита было проведено тестирование, в котором выявлены преимущества нового решения: новый инструмент гораздо производительней, а также лучше работает с памятью системы [8, 9].

Проведение аудита безопасности, а также его публикация демонстрируют заинтересованность команды разработки *Matrix* в развитии своего продукта путём создания и поддержки криптографических библиотек и готовых реализаций мессенджеров в виде клиента *Element* и сервера *Synapse*, а также поддержки пользовательских решений.

Рассматривая данный протокол, стоит заметить, что преимуществом использования его функционала является серверная реализация. Большинство хостов *Matrix*, используемых внутри ее сети, являются пользовательскими. Они соединяются в федерацию, образуя единую сеть хостов, и позволяют пользователям, зарегистрированным на разных серверах, общаться друг с другом вне зависимости от места регистрации. То, как происходит взаимодействие клиентов, продемонстрировано при помощи диаграммы состояний на рис. 3 и цветами размечено, как сообщения передаются между пользователями. Сервер может быть создан и для частного пользования, отдельно от федеративной сети, что может быть полезно для компаний, рассматривающих корпоративное безопасное общение своих сотрудников.

Дополнительными возможностями протокола является создание соединений, называемых мостами, между клиентом *Matrix* и клиентом стороннего приложения (например, *Skype* или *WhatsApp*), что позволяет создать на одном приложении универсальный мессенджер для связи [10].

Данные функции протокола *Matrix* можно наблюдать и в других инструментах мгновенного обмена сообщениями. Протокол *XMPP*, в котором также можно реализовать свой сервер и настроить взаимодействие с другими клиентами, отличается обеспечением безопасности. Протокол использует инструменты шифрования трафика *TLS*, но при этом не шифрует само сообщение [11]. Такой подход может привести к потере конфиденциальной информации, из-за чего вместе с протоколом *XMPP* необходимо использовать сторонние криптографические инструменты и библиотеки.

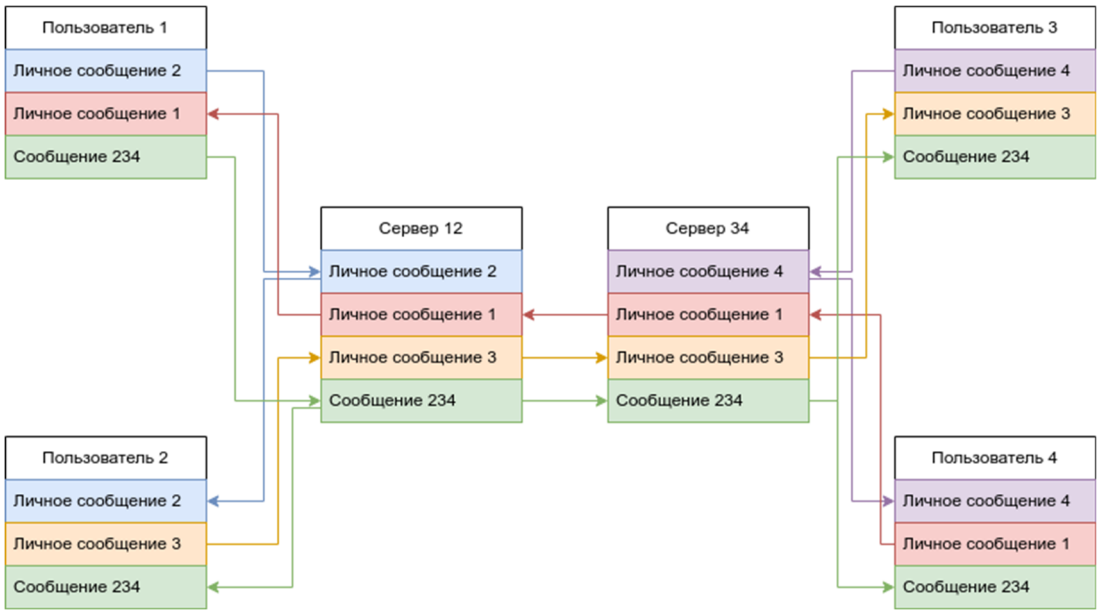

Рис. 3. Диаграмма состояний федеративной сети *Matrix*

Протокол *Matrix* является удобным вариантом для реализации средств общения пользователей сети друг с другом, а также для общения целой группы, при этом не жертвуя производительностью и конфиденциальностью.

Данные инструменты действительны против внешних злоумышленников и направлены на препятствование быстрому получению персональных данных и конфиденциальных переписок пользователей и не рассматривают внутренних злоумышленников. Угрозы, которые строятся на доверии пользователей друг к другу, решаются не криптографическими методами.

Обсуждение

Команда разработчиков протокола предоставляет собственные реализации сервера и клиента, использующие инструментарий *Matrix*. Клиент *Element* обновляется, расширяя свои возможности в обмене сообщениями, а также в нем ликвидируются обнаруживающиеся уязвимости. Он имеет простой интерфейс с возможностью управления свойствами через web-интерфейс или настольное приложение.

Сервер *Synapse* управляется непосредственно через файл конфигурации, в котором указаны необходимые параметры для поддержания сервера в работоспособном состоянии. Он не имеет в своем функционале простого взаимодействия и для изменений каких-либо параметров требует ручного изменения и перезапуска системы. Для решения данной проблемы можно создать собственный сервер, позволяющий управлять конфигурацией сервера протокола *Matrix* через интерфейс, как это происходит с клиентом *Element*, а также создать автоматизированную развертку на пользовательской машине с конфигурированием параметров хранения данных и логирования, а также с возможностью удобного чтения и записи получаемых данных непосредственно в реализуемом решении.

Также создание web-интерфейса для удобства обращения с сервером позволяло администраторам собственного сервера управлять его возможностями дистанционно, без необходимости изменять конфигурационные файлы, как это сделано в решении *Synapse*. Схема реализации данного подхода управления сервером продемонстрирована на рис. 4.

В результате дальнейшего исследования предметной области будет создаваться программная реализация приложения, реализующего данные возможности. При этом продемонстрированный функционал может быть дополнен новыми опциями.

Рис. 4. Реализация сервера с web-интерфейсом

Заключение

В результате проведенного исследования были выделены характеристики протоколов мгновенного обмена сообщениями и разобран криптографический примитив, на базе которого проектируются современные инструменты шифрования сообщений. Одним из таких протоколов, реализующих алгоритм двойного храповика, является *Matrix* – платформа, при помощи которой создаются клиенты, способные взаимодействовать с клиентами, созданными на базе других протоколов мгновенного обмена сообщениями. *Matrix* продолжает совершенствоваться и обновляться, что говорит о высокой поддержке со стороны разработчиков, вследствие чего данный криптографический протокол можно применять для создания собственных мощных и безопасных решений для обмена сообщениями. Дальнейшее изучение данной предметной области будет основано на предложенном решении по созданию серверной реализации протокола *Matrix* с графическим или web-интерфейсом, что снизило бы порог вхождения в работе с серверной реализацией протокола.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Басыня Е. А. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предприятия / Е. А. Басыня. - Текст : непосредственный // Защита информации. Инсайд . - 2021. - № 5 (101). - С. 16-25.

2. Тихонова А.Д., Методы обеспечения конфиденциальности в современных системах обмена мгновенными сообщениями / Тихонова А.Д., Теплюк П.А. // Программно-техническое обеспечение автоматизированных систем(ПТОАС-2020) Барнаул, 16 декабря 2020 г. - С. 123-128.

3. Кених Н.В. Методы защиты информации / Кених Н.В. // Наука в современном обществе: закономерности и тенденции развития, Уфа, 28 сентября 2016 г. - №1. - С. 30-32.

4. Куваев А.В. Особенности моделирования и реализации сквозного шифрования / Куваев А.В., Хорошко М.Б. // Моделирование. Фундаментальные исследования, теория, методы и средства. Новочеркасск, 30-31 июля 2018 г. С. 66-70.

5. Карондеев А. М., Исследование защищенности пользовательских данных мобильных приложений на примере мессенджера WhatsApp / Карондеев А. М., Клюев Д. В. // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. -2019. -№07. -С. 88-93.

6. Ефромеев Н.М. Обзор протоколов обмена мгновенными сообщениями для защищённого корпоративного общения / Ефромеев Н.М., Хорошеев В.О., Ефромеева Е.В. // Информационные технологии и автоматизация управления, Омск, 29-30 мая 2020 года, - С. 58-63.

7. Olm: криптографический храповик. – URL: https://gitlab.matrix.org/matrix-org/olm/-/blob/master/docs/olm.md (дата обращения 29.04.2023).

8. Vodozemac - отчет об аудите безопасности, 30 марта 2022 г. – URL: https://matrix.org/media/Least%20Authority%20-%20Matrix%20vodozemac%20Final%20Audit%20Report.pdf (дата обращения 28.04.2023).

9. Независимый публичный аудит «Vodozemac», нативной эталонной реализации сквозного шифрования Matrix на Rust. – URL: https://matrix.org/blog/2022/05/16/independent-public-audit-of-vodozemac-a-native-rust-reference-implementation-of-matrix-end-to-end-encryption (дата обращения 29.04.2023).

10. Мосты. – URL: https://matrix.org/bridges/ (дата обращения 29.04.2023).

11. RFC7590: использование безопасности транспортного уровня (TLS) в расширяемом протоколе обмена сообщениями и присутствия (XMPP). URL: https://xmpp.org/rfcs/#7590 (дата обращения 29.04.2023).