УДК 00.004.056

АНАЛИЗ БЕЗОПАСНОСТИ И КРИПТОГРАФИИ ПРОТОКОЛА MATRIX

Н.М. Павлов[1]

[1]*Саратовский государственный технологический университет им. Гагарина Ю.А, г. Саратов*
e-mail: nik.pavlov.9191@inbox.ru

Аннотация

В статье анализируется протокол MATRIX с точки зрения безопасности и криптографии с общим описанием его работы. Приводится описание атак и их предотвращение. Описываются алгоритмы Olm/Megolm и ключи шифрования.

Ключевые слова: информационная безопасность, криптография, мгновенный обмен сообщениями, протокол MATRIX, открытое программное обеспечение (ПО).

Введение

В Интернете всегда будет оставаться вопрос защиты информации и безопасности пользователей. Существуют десятки протоколов для общения в сети. Много популярных мессенджеров используют закрытые разработки, скрытые от изучения. Такие продукты поставляются без исходников, от чего проблема в безопасности и наличии возможных уязвимостей остаётся опасной. Однако, от этого недостатка избавлены протоколы с публичными алгоритмами. MATRIX это открытый протокол обмена сообщениями с шифрованием [3]. На основе него работает мессенджер Element и похожие на него [4]. Защита пересылаемых сообщений от получателя(ей) и отправителя(ей) работает в MATRIX благодаря механизму Olm/Megolm, работа которых основана на двойном храповике, а также использованию ключей ED25519 и Curve25519.

1. Механизм работы двойного храповика

Алгоритм, использует симметричное и ассиметричное шифрование, где вторым генерируется секретный ключ, а после из самого значения создаются: *root key* и *session key 1*, на шифрования сообщений [2]. При отправке сообщения, функция “KDF” создает два ключа: *session key 2* и *message key 1*. Последним шифруется сообщение, а после им же расшифровывается на другой стороне. Если сообщение отправляет собеседник, то при помощи ассиметричного шифрования генерируется новый *root key*, и далее функциями генерируются *session key* и *message key*, как на рисунке 1.

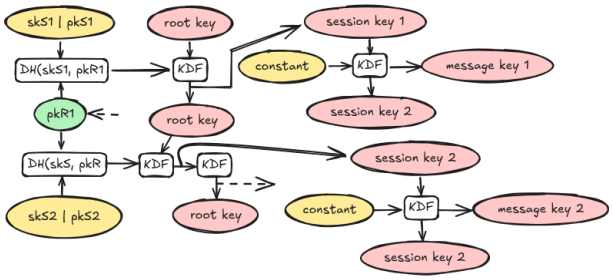

Рисунок 1 – Общая схема алгоритма двойного храповика

2. Проблемы сквозного шифрования, которые решаются в MATRIX

Атака – *человек посередине*. Это ситуация, когда кракер [5] захватывает под свой контроль канал связи между хостами и может подменить открытый ключ. Чтобы не дать себя обнаружить, после дешифровки сообщения он может зашифровать его ключом, который он разделяет с фактическим получателем, или его открытым ключом и снова отправить сообщение. Концептуально схему атаки можно увидеть на рисунке 2.

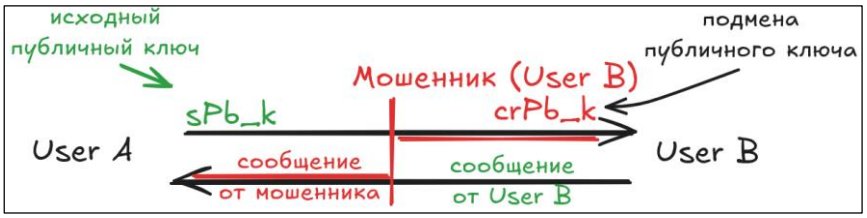

Рисунок 2 – MITM атака

Для её устранения в MATRIX используется аутентификация, через центры сертификации (т.н. Let's Encrypt). Помимо этого, стороны сравнивают свои “отпечатки открытых ключей” с использованием внешнего канала связи, который гарантирует целостность и её аутентичность. Если отпечатки совпадают, всё в порядке.

Атака – *безопасность конечных точек*. Это недостаток, связанный с “компрометацией устройства” – то есть его взлом, с целью украсть ключи. Проблема решается даже не протоколом, а клиентом (т.н Element). В нём есть возможность запрета на создание скриншотов, установка отдельного PIN-кода для входа в профиль. Стоит в целом уделить внимание защите гаджета с помощью программных или иных методов (использовать только необходимое и желательно открытое ПО), так например пользоваться виртуальной клавиатурой, которая не запрашивает специфические привилегии и не может содержать потенциальных клавиатурных шпионов.

Атака *бэкдором* представляет дефект алгоритма намеренно встраиваемый кракером и позволяет получить доступ к данным. Простой метод обхода этой угрозы – использование проверенных клиентов и серверов MATRIX. В том числе важно подбирать такие решения, в которых частый аудит. Самый удачный и надежный клиент – Element, а для серверной части подходит Synapse или Dendrite.

3. Olm/Megolm механизмы

Olm реализует стандартный двойной храповик и используется для шифрования коммуникации между двумя пользователями (один-на-один).

Megolm это расширенная версия алгоритма Olm, предназначенная для шифрования сообщений между большим количеством клиентов. Данная модификация необходима для синхронизации состояний храповика на всех клиентах, находящихся в одном пространстве сети, называемом комнатой.

Эти два механизма реализованы библиотекой Vodozemac [7].

4. Ключи протокола MATRIX для работы сквозного шифрования

ED25519-ключ – позволяет идентифицировать устройства (со стороны клиента). Используется пара ключей: приватный только на устройстве, а публичный в сети MATRIX [1].

Curve25519-ключ – создаёт общий секретный ключ. Состоит из пары ключей: приватный – для установления сеанса связи с устройством и публичный – публикуемый в сети MATRIX.

Curve25519-одноразовый ключ – для установки сеансов связи Olm с разными пользователями в сети.

ED25519 Megolm. Пара ключей для подписи сообщений через сеанс Megolm и для аутентификации отправителя.

5. Практический анализ обеспечения шифрования сети MATRIX

Чтобы убедиться, что шифрование действительно функционирует между клиентами в сети, проверим это через инструмент анализа трафика – Wireshark [6]. Напишем любое сообщение с клиента нашему собеседнику в уже настроенной заранее комнате как на рисунке 3

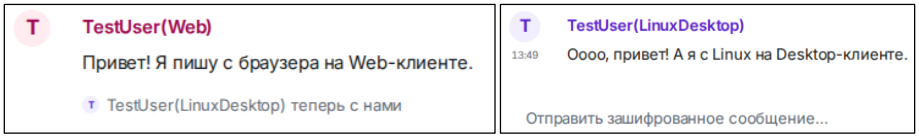

Рисунок 3 – Отправка сообщения с клиентов

Теперь проанализируем шифрование TLS/SSL и сквозное шифрование (E2EE) в сети. После выбора нужного сетевого интерфейса в поле фильтра (display filter) укажем известный IP-адрес домена matrix.org и выполним запрос. Увидем следующий список пакетов как на рисунке 4.

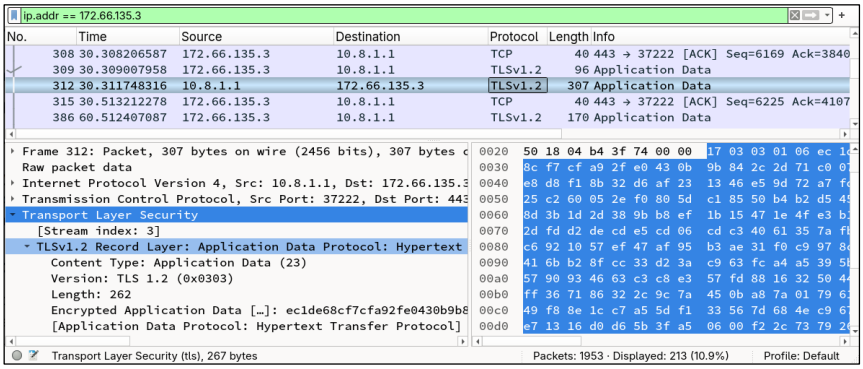

Рисунок 4 – Анализ зашифрованного пакета в Wireshark

Из этой информации можно сделать следующий вывод, что действительно используется TLS версии 1.2. Помимо этого указан тип данных “Encryption Application Data”, а значит, шифрование транспортного уровня работает и содержимое сообщений скрыто. Также можно убедиться в этом, если посмотреть на текст пакета как на рисунке 5. Выделенная области справа после hex-строк вида как “абракадабра” – это и есть зашифрованное содержимое. Мы не можем прочитать сообщения, так как они зашифрованы ключами, хранящимися только у участников чата.

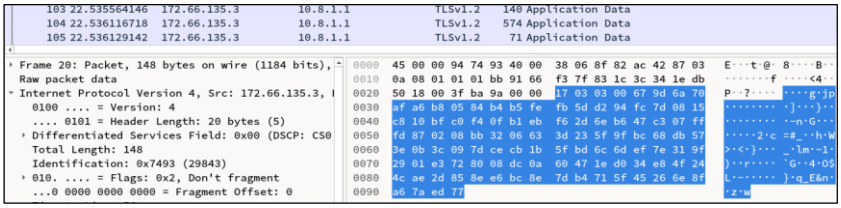

Рисунок 5 – Зашифрованное содержимое

Заключение

В данной статье рассматривалась технология MATRIX, с точки зрения безопасности и криптографии. Стоял вопрос о защите информации и безопасности пользователя от компрометаций в сети Интернет. Была описана работа механизма двойного храповика. Был проведён разбор основных ключей, применяемых в клиентах и самой сети, а также основные атаки, которые предотвращаются в протоколе. Помимо этого, с практической стороны была доказана работа шифрования через Wireshark.

Можно сделать вывод, что в современное время любой может обеспечить себе необходимый уровень защиты и безопасность в сети, на основе открытых технологий, которые не скрывают свои тонкости работы и механизмы шифрования.

Список использованных источников

1. MATRIX. Документация по реализации сквозного шифрования – URL: https://matrix.org/docs/matrix-concepts/end-to-end-encryption/ (дата обращения: 19.03.2026).

2. Signal. Double Ratchet Algorithm – URL: https://signal.org/docs/specifications /doubleratchet/ (дата обращения: 20.03.2026).

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

4. Список программ-клиентов для MATRIX – URL: https://matrix.org/ ecosystem/clients/ (дата обращения: 21.03.2026).

5. Хакеры или кракеры, а кто это? – URL: https://www.crime-research.org/library/hack22.htm (дата обращения: 19.04.2026).

6. Wireshark. Подробное руководство по использованию – URL: https://habr.com/ ru/articles/735866/ (дата обращения: 19.04.2026).

7. Vodozemac. Официальная документация – URL: https://matrix-org.github.io/ vodozemac/vodozemac/index.html (дата обращения: 19.04.2026).

SECURITY AND CRYPTOGRAPHY ANALYSIS OF THE MATRIX PROTOCOL

N.M. Pavlov[1]

[1]Saratov State Technological University named after Yu.A. Gagarin SSTU, Saratov
e-mail: nik.pavlov.9191@inbox.ru

Abstract

The article analyzes the MATRIX protocol from the point of view of security and cryptography with a general description of its operation. The attacks are described and prevented. The Olm/Megolm algorithms and encryption keys are described.

Keywords: information security, cryptography, instant messaging, MATRIX protocol, open source software.