УДК 004.773

О. С. Осинцев[1]*

Системы межпротокольной коммуникации клиентов с использованием технологии мостовой передачи

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: osincevoleg@mail.ru

Аннотация. Коммуникация пользователей внутри сети является неотъемлемой частью жизни пользователей сети интернет. При этом с целью уменьшения рисков утраты конфиденциальной информации и нарушения тайны переписки разработчиками платформ обеспечиваются безопасность систем и анализ угроз. Взаимодействие клиентов, использующих разные протоколы мгновенного обмена сообщениями, осуществляется третьими сторонами, добавляя факт доверия дополнительной стороны и увеличивая при этом риск нарушения безопасности. В данной работе рассматриваются системы межпротокольной коммуникации клиентов с использованием технологии мостовой передачи. Цель данного исследования заключается в изучении существующих подходов к обеспечению взаимодействия между различными протоколами обмена сообщениями, оценке их функциональных возможностей и влияния на уровень защищенности передаваемой информации. В ходе исследования были определены основные направления дальнейшего совершенствования технологий мостовой коммуникации, позволяющих интегрировать разные протоколы обмена сообщениями и унифицировать их в единую систему.

Ключевые слова: межпротокольная коммуникация, matrix bridge, XMPP bridge, CRM, мессенджер-бот, мостовая передача

O. S. Osincev[1]*

Interprotocol Communication Systems for Clients Using Bridge Transmission Technology

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

Annotation. Communication between users within the network is an integral part of the life of Internet users. At the same time, in order to reduce the risks of losing confidential information and violating the privacy of correspondence, platform developers ensure system security and threat analysis. Clients using different instant messaging protocols interact with third parties, adding additional party trust and increasing the risk of security breaches. This paper discusses interprotocol client communication systems using bridged transmission technology. The purpose of this study is to study existing approaches to ensuring interaction between various messaging protocols, assessing their functionality and impact on the level of security of transmitted information. The study identified the main directions for further improvement of bridge communication technologies, allowing for the integration of different messaging protocols and unification of them into a single system.

Keywords: interprotocol communication, matrix bridge, XMPP bridge, CRM, messenger bot, bridge transmission

Введение

Современные мессенджеры и сервисы мгновенных сообщений позволяют пользователям интернета оперативно обмениваться большими объемами информации в виде текста, изображений и видео на большие расстояния, тратя на передачу данных минимум времени. Хотя существует множество протоколов, обеспечивающих безопасную коммуникацию внутри отдельных сетей, взаимодействие между пользователями разных мессенджеров в стандартной конфигурации затруднено, так как «из коробки» кроссплатформенный обмен сообщениями не предусмотрен.

Крупные компании не заинтересованы в создании межпротокольной связи между различными мессенджерами, так как разработка таких систем не принесёт им дополнительных преимуществ. Увеличение аудитории отдельно взятого мессенджера или повышение эффективности бизнеса при этом не будет достигнуто. Поскольку у многих пользователей уже установлено несколько приложений для обмена сообщениями, объединение их в одну систему не приведёт к росту доходов компаний [1].

Для пользователей мессенджеров, напротив, использование нескольких различных систем для коммуникации с другими пользователями является менее эффективным подходом. Для общения людей используются разные приложения обмена сообщениями, которые потребляют дополнительные ресурсы устройств и могут быть неудобны в использовании. Для решения данной проблемы были разработаны технологии межпротокольной коммуникации [2-3].

Возможны следующие подходы к интеграции между пользователями разных мессенджеров:

– использование ботов в мессенджерах для пересылки сообщений;

– CRM-системы для централизованного хранения и обмена данными;

– мостовые технологии на базе протоколов Matrix и XMPP, позволяющие преодолевать ограничения протоколов.

Каждый из этих подходов имеет свои преимущества и недостатки.

Системы межпротокольной коммуникации

Обеспечение конфиденциальности передаваемых сообщений между пользователями различных протоколов связи является важной задачей для обеспечения кибербезопасности. При этом решение задачи взаимодействия нескольких протоколов предполагает наличие промежуточного звена в виде системы межпротокольной передачи данных, которая должна обеспечивать декодирование сообщений, полученных по одному протоколу, временное хранение сообщения в открытом виде для последующей передачи по другому протоколу, а также шифрование сообщения и передачу по второму протоколу связи, беря на себя функции обеспечения взаимодействия несовместимых каналов связи. При этом критически важно обеспечить надежную защиту данных на этапе их временного хранения в открытом виде.

Мессенджер-бот – проприетарная система агрегации сообщений, направленная на предоставление возможности коммуникации клиентов, использующих различные протоколы. Функционал позволяет получать и перенаправлять пользователям не только сообщения из различных мессенджеров, но и из различных новостных каналов, почтовых рассылок и CRM.

Существует множество развернутых мессенджер-ботов. В основном данные системы коммерциализированы и предоставляют свои услуги по подписочной системе, в результате чего передаваемые сообщения проходят через централизованное хранилище, и безопасность и конфиденциальность данных зависят от самого поставщика услуг [4-5].

CRM (англ. Customer Relationship Management) – система управления взаимоотношениями с клиентами, представляющая собой проприетарную платформу для управления взаимоотношениями с клиентами посредством агрегации сообщений и использования мессенджеров и телефонии в качестве каналов коммуникации [6]. Эта технология имеет определенное сходство с мессенджер-ботом, поскольку предоставляет аналогичные функциональные возможности пользователям. Однако CRM отличается рядом особенностей, благодаря которым обеспечивает более широкий функционал, дающий возможность управления взаимоотношениями с клиентами [7].

Разработчики технологии CRM предоставляют возможность развернуть собственную внутреннюю платформу для системы управления взаимоотношениями с клиентами. Это дает возможность коммерческой организации обеспечить хранение и обработку переписок между клиентом и менеджером исключительно на локальных ресурсах предприятия. Таким образом, достигается более высокий уровень защиты персональных данных по сравнению с использованием внешних сервисов, где данные могут быть доступны третьим сторонам.

Данная технология обеспечивает использование дополнительных возможностей коммуникации, отличных от обычных мессенджеров, таких как телефония, почта и других. Это позволяет расширить возможности управления отношениями с большим числом существующих и потенциальных клиентов [8, 9].

Система CRM предоставляет мощный инструментарий для коммерческих компаний и взаимодействия между организацией, предоставляющей услуги, и клиентом, который получает услугу. Доступ к системам может организовывать сам разработчик, как предоставляя услуги к облачному сервису, так и предоставлять возможность самостоятельного развертывания на серверных мощностях компании.

Использование облачных сервисов позволяет пользователям существенно снизить собственные затраты и усилия по обеспечению безопасности информационных систем и инфраструктуры [10]. Владельцы облачных платформ берут на себя ответственность за регулярное обновление систем защиты, мониторинг угроз и предотвращение инцидентов. Однако перекладывание функций кибербезопасности на внешние компании может привести к снижению контроля над данными со стороны пользователей. Кроме того, полная зависимость от облачного провайдера увеличивает риск сбоев в работе сервисов и невозможности опе-

ративного доступа к данным. Персональная информация компаний и пользователей хранится на серверах облачных компаний, что увеличивает потенциальную уязвимость в случае инцидентов безопасности у поставщиков облачных услуг [11].

Развертка собственного сервера возлагает ответственность за функции кибербезопасности на компанию и дает возможность хранить и обрабатывать все данные на своих мощностях. Данное решение может эффективно подойти для корпоративной сети компании и делового общения, но развертывание для использования в качестве мессенджера может повлечь за собой нарушение конфиденциальности переписки между пользователями [2].

Мостовые технологии – специальные модули, разрабатываемые в рамках протоколов мгновенного обмена сообщениями, разворачиваемые на серверных мощностях. Они позволяют клиентам мессенджера с мостом общаться с пользователями других протоколов коммуникации как легитимные участники сети. Развитием данных технологий занимаются компании matrix.org и xmpp.org.

Протоколы Matrix и XMPP создавались как решения с открытым исходным кодом и с современными и уникальными технологиями: федеративная коммуникация, децентрализация и масштабирование, сквозное шифрование, межпротокольность [12]. Компании предоставляют возможность развертки собственных серверов и клиентов, что позволит пользователям создавать свои коммуникационные сети на локальном уровне для коммуникации внутри небольшой группы или использовать федеративную сеть для коммуникации со всеми клиентами описанных протоколов [14].

Мост развертывается на существующем Matrix- или XMPP-сервере и поддерживается системным администратором конкретного узла сети. В данном случае сервер выступает в роли клиента для отличного протокола и в качестве сервера – для своей сети. Когда сообщение отправляется, на мосту оно расшифровывается одним протоколом и зашифровывается другим для передачи внутри другой сети (рис. 1). Для защиты открытых данных в момент конвертации сообщения оно, по спецификациям протокола Matrix, может шифроваться сквозным шифрованием, тем самым скрывая его от администратора узла [15].

Технология интеграции между различными системами обмена сообщениями на основе протокола Matrix будет обеспечивать более высокий уровень конфиденциальности по сравнению с решениями, основанными на ботах или CRM. Это достигается за счет применения сквозного шифрования на узле мостовой системы, благодаря чему невозможен просмотр или извлечение содержимого передаваемых сообщений. При этом от хоста потребуется высокий уровень доверия для обеспечения надежной передачи сообщений между клиентами разных протоколов.

При данном подходе пользователю не нужно поддерживать в постоянно работоспособном состоянии мост для коммуникации с другими пользователями.

Достаточно иметь один мост с включенными параметрами безопасности, чтобы вести переписки клиентов с пользователями других протоколов. Но для

развертывания инфраструктуры потребуется высокий уровень навыка настройки, что может быть затруднительным для рядового пользователя.

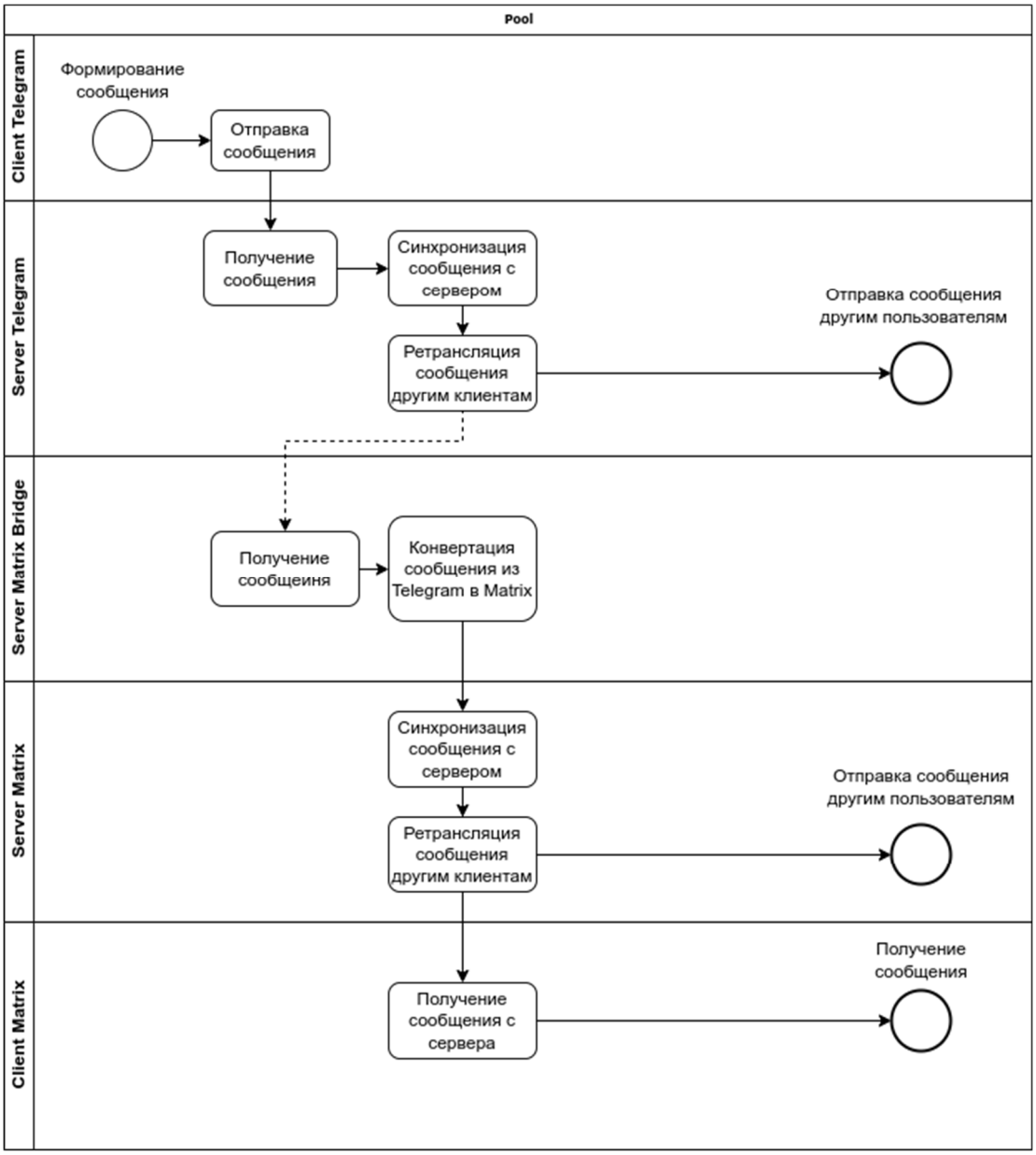

Рис. 1. BPMN-диаграмма движения

Мостовая технология развивается и имеет ограниченность в технологических функциях. На данный момент протокол Matrix предоставляет возможность коммуникации с приложениями Telegram, WhatsApp, Signal, Skype и другими. Многие мосты поддерживаются разработчиками открытого программного обеспечения и не имеют полных функциональных возможностей, таких как сквозное шифрование. Но они продолжают развиваться и дополняться функциями по спецификации протокола Matrix.

Заключение

В ходе исследования были рассмотрены системы межпротокольной коммуникации, их возможности и оценка перспектив использования для консолидации разных мессенджеров в единую коммуникационную сеть. Протокол Matrix и XMPP имеют встраиваемые в сервер инструменты, осуществляющие трансляцию сообщений в другие мессенджеры, при этом имеют возможность сквозного шифрования трафика в момент обмена сообщениями через мост, что позволяет сохранить конфиденциальность передаваемой через протоколы информации. В этом состоит преимущество данных систем от CRM или мессенджер-бота, т.к. в них сообщение обрабатывается в открытом виде, что потенциально может повлечь большую утечку переписок в массовых коммуникациях.

Дальнейшие исследования данной области помогут усовершенствовать существующие программные решения и будут способствовать созданию новых инструментов, связывающих разные протоколы в единую коммуникационную сеть.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Басыня Е.А. Метод интеллектуально-адаптивного управления информационной инфраструктурой предприятия / Басыня Е.А. // Информационные Технологии. – 2020. – Т.26 №3. – С. 185-191.

2. Басыня Е.А. Автоматизированная установка и конфигурирование серверных решений / Басыня Е.А., Лукина М.С. // Современные материалы, техника и технологии. – 2016. – №2(5). – С. 21-26.

3. Басыня Е.А. Безопасность и анонимизация автоматизированной настройки серверных решений / Басыня Е.А., Лукина М.С. // ГНИИ «НАЦРАЗВИТИЕ». – 2016. – С. 69-76.

4. Чунаева А.А. Агрегатор систем сообщений / Чунаева А.А. // Энергия-2021. – 2021. – С. 67.

5. Шигаев Д.К. Разработка архитектуры веб-приложения для сбора и обработки сообщений в один агрегатор / Шигаев Д.К., Жулева С.Ю. // Математическое и программное обеспечение вычислительных систем. – 2022. – С. 6-9.

6. Тухватуллин И.Д. CRM-система / Тухватуллин И.Д. // Современные условия взаимодействия науки и техники. – 2017. - №1. – С. 88-90.

7. Bourreau M. Horizontal and vertical interoperability in the DMA / Bourreau M., Kramer J. // Centre On Regulation in Europe. – 2023. – С. 1-36.

8. Софронова Н.В. CRM-система в практике организационного управления университетом / Софронова Н.В. // Цифровая трансорфация образования: актуальные проблемы, опыт, решения. – 2021. – №4. – С. 175-185.

9. Золина А.А. CRM-система как инструмент оптимизации бизнес-процессов компании / Золина А.А., Ильина О.П. // Цифровая трансформация в экономике и управлении. – 2021. – С. 64-74.

10. Дедков Д.А. Безопасность CRM-систем / Дедков Д.А., Ремесник Е.С. // Проблемы информационной безопасности социально-экономических систем. – 2021. – С. 58-59.

11. Новикова А.С. Проблемы защиты данных при применении облачных систем / Новикова А.С., Фомина А.В. // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. – 2020. – С. 22-26.

12. Mautrix-bridges end-to-bridge encryption. – URL:https://docs.mau.fi/bridges/general/end-to-bridge-encryption.html (дата обращения: 20.04.2024).

13. Schipper G.C. Forensis Analysis of Artifacts in the Matrix Protocol and Riot.IM application / Schipper G.C., Seelt R., Le-Khac N. // Forensic Science International Digital Investigation. – 2021. – С. 1-11.

14. Osipov D.L. Development of a Server Software Module for Protected Data Sharing on the Internet / Osipov D.L., Tebueva F.B., Ryabtsev S.S., Struchkov I.V. // Wireless Personal Communications. – 2019. – С. 1-10.
15. XMPP protocol. – URL : https://xmpp.org/ (дата обращения: 20.04.2024).

© О. С. Осинцев, 2024