Метод передачи сообщений, с использованием лучших способов организации обмена данными и криптографических протоколов обмена мгновенными сообщениями с использованием сквозного шифрования

А.С. Дмитриев, Д.О. Холкин, М.А. Маслова

Волгоградский государственный технический университет.

Аннотация: В данной статье предлагается разработка метода передачи защищенных сообщений, используя комбинацию лучших способов организации обмена данными и криптографических протоколов обмена мгновенными сообщениями с использованием сквозного шифрования. Рассмотрены способы организации приложения с использованием одноранговой сети и при помощи клиент-серверной архитектуры. Проведен анализ популярных протоколов передачи мгновенных сообщений с использованием сквозного шифрования. Описаны программные компоненты приложения, основанного на разработанном методе.

Ключевые слова: мессенджер, сквозное шифрование, криптографический протокол, мгновенные сообщения, одноранговая сеть, клиент-сервер.

В современных условиях развития общества роль цифровых технологий в различных отраслях неуклонно растет. Значимость информации, хранящейся на носителях, обрабатываемой приложениями или передаваемой по каналам связи для организаций и частных лиц, выходит на передний план. Так, обмен мгновенными сообщениями становится неотъемлемой частью социальной и деловой жизни. По данным Statista, компании, специализирующейся на рыночных и потребительских данных, аудитория самого популярного мессенджера WhatsApp в 2020 году составила более 2 миллиардов пользователей [1]. Основная проблема систем обмена мгновенными сообщениями заключается в том, что передаваемая информация может быть перехвачена злоумышленником, соответственно

нарушается конфиденциальность личных данных пользователя, что может привести к неприятным последствиям.

Повысить безопасность передаваемых данных можно, используя шифрование данных. С развитием криптографических алгоритмов для систем передач мгновенных сообщений, пришли к использованию алгоритмов на основе метода сквозного шифрования. Суть сквозного шифрования заключается в том, что исходное сообщение обрабатывается на стороне устройства отправителя, в зашифрованном виде передается по каналам связи к получателю, и только на устройстве получателя расшифровывается в исходное сообщение. Таким образом, на всем маршруте передачи данных между устройствами сообщение остается защищено от атак злоумышленника.

В данной статье предлагается разработка метода передачи защищенных сообщений, используя комбинацию лучших способов организации передачи данных и криптографических протоколов обмена мгновенными сообщениями с использованием сквозного шифрования.

Был произведен разбор и анализ существующих способов организации сетевой архитектуры приложения, а также криптографических протоколов обмена мгновенными сообщениями с использованием сквозного шифрования.

В настоящее время существует два основных подхода к организации сетевой архитектуры приложения, а именно - одноранговые (далее P2P) сети и клиент-серверная архитектура.

Одноранговая сеть – это распределенная архитектура приложения, которая разделяет задачи между узлами. Узлы имеют одинаковые привилегии в приложении и образуют сеть равносильных узлов [2]. Основным свойством P2P сети является децентрализация, поведение системы определяется коллективными действиями одноранговых узлов,

централизованный пункт управления отсутствует. Однако некоторые системы используют централизованный сервер аутентификации.

Клиент-серверная архитектура представляет собой связь между сервером и клиентами, подключенными к нему. В большинстве клиент-серверных сред обработка данных выполняется сервером, а результаты возвращаются клиентам, что делается для ускорения скорости работы системы и снижения нагрузки на клиентскую машину.

Основным свойством клиент-серверной архитектуры является наличие централизованного сервера и базы данных, управляемой сервером. Централизация приводит к ряду недостатков, например, при неисправности сервера, неисправной становится вся вычислительная система. Для решения этой проблемы можно использовать множество серверов и балансировщик нагрузки, что, однако, повышает стоимость серверного оборудования и сложность его обслуживания. Другим недостатком является то, что обмен сообщениями между клиентом и сервером приводит ко множеству проблем безопасности. Становятся доступными многие виды атак на передаваемые данные, например, человек посередине (далее MitM). Благодаря тому, что весь обмен информации проходит через сервер и хранится на нем, возникают и следующие проблемы: возможность физического ущерба серверу, угрозы для получения доступа к нему и вирусные атаки.

Одним из ключевых достоинств клиент-серверной архитектуры является простота организации связи между клиентами приложения, благодаря единому серверу аутентификации. Благодаря посреднику между клиентами в виде сервера, у клиентов отпадает необходимость связи друг с другом напрямую для передачи данных, что избавляет от проблем подключения, например, в случае изменения IP-адреса одного из собеседников.

Это достоинство клиент-серверной архитектуры является одним из главных недостатков одноранговой сети. Однако эту проблему можно решить, используя структурированную P2P сеть.

Структурированная сеть – это «сеть, в которой узлы совместно хранят информацию о том, как достичь всех других узлов сети» [3]. По сравнению с неструктурированными сетями, структурированные обеспечивают ограничение на необходимое количество запросов для нахождения любого объекта в сети.

Одним из способов организации структурированной одноранговой сети является использование распределенной хэш-таблицы (DHT) [4]. Распределенная хэш-таблица представляет собой структурированную сеть, использующую маршрутизацию по ключам для операций ввода и получения индекса, в котором каждому равноправному пользователю присваивается часть DHT-индекса. В системах P2P на базе DHT, узлы организуются в соответствии с реализацией DHT для формирования графа коммуникаций с оптимальным компромиссом диаметра/степени графа. Каждый узел сети поддерживает в таблице маршрутизации адреса других узлов одного и того же DHT, отсортированные в соответствии с определенными критериями.

Использование DHT вместо централизованного сервера аутентификации позволяет поддерживать следующие, важные для мессенджеров с защищенной передачей данных, свойства: децентрализация – отсутствует необходимость центрального сервера, который может быть уязвим для ряда атак на данные пользователей; масштабируемость – приложение будет одинаково эффективно функционировать вне зависимости от количества пользователей сети; отказоустойчивость – при отключении некоторых узлов сети, остальная сеть будет работать, как и прежде.

Таким образом, исходя из достоинств и недостатков рассмотренных методов, для использования в мессенджере с поддержкой сквозного

шифрования, будет использована одноранговая сеть с применением распределенной хэш-таблицы, тем самым, позволяя отказаться от уязвимого централизованного сервера и подключать узлы напрямую друг к другу.

Был проведен анализ существующих криптографических протоколов передачи мгновенных сообщений с поддержкой сквозного шифрования. Основными критериями отбора были: гарантия криптографического свойства – совершенной прямой секретности (PFS), открытость стандарта и наличие независимого аудита протокола. По совокупности критериев были выбраны протоколы Signal и MTProto. Оба эти протокола прошли независимый аудит [5 – 7].

Так, по данным исследования [5], в протоколе MTProto используется слабая версия протокола Диффи-Хеллмана, предпочтительнее было бы использовать метод эллиптических кривых. Так же, протокол нарушает свойство PFS, так как промежуточные ключи, которыми шифруются сообщения, меняются раз в 100 сообщений или раз в неделю. В связи с чем, при компрометации одного ключа, злоумышленник сможет расшифровать до 100 сообщений.

В исследовании [6] протокола Signal автор пришел к следующей проблеме в реализации протокола Signal в одноименном приложении для ОС Android: не соблюдается криптографическое свойство отрицания. Несмотря на то, что для шифрования сообщений используется симметричная криптография, отрицание не выполняется, так как пользователь все еще аутентифицируется на сервере и, следовательно, не может отрицать участие в разговоре.

В крупном аудите [7] протокола Signal отметили следующие существующие слабые места протокола:

- используется одинаковый ключ для подписи Ed25519 и Curve25519 Диффи-Хеллмана. Протокол использует тот же ключ *ik* для соглашения

Диффи-Хеллмана и для подписания среднесрочных предварительных ключей. Однако, исследование [8] доказывает безопасность данной схемы.

- дешифровка сообщений не по порядку. В случае, если сообщения приходят получателю не в порядке их отправки, пользователи вынуждены хранить цепочки ключей шифрования, что снижает безопасность пересылки сообщений.

В заключение, авторы пришли к выводу о том, что криптографическое ядро протокола Signal обеспечивает стандартные свойства безопасности. Протокол обеспечивает секретность и аутентификацию ключей сообщений, даже при различных сценариях компрометации со стороны противника, таких, как прямая секретность (FS). При правильном использовании Signal может достичь пост-скомпрометированной безопасности (post-compromise security), которая имеет существенные преимущества перед FS, как это описано в [9].

Стоит отметить, что в текущих реализациях мессенджеров, основанных на протоколе Signal, в качестве идентификатора пользователя используется телефонный номер. В связи с этим снижается анонимность пользователей, а также становится возможным не только узнать, пользуется ли мессенджером определенно взятый пользователь, но и собрать базу данных всех номеров, зарегистрированных в системе [10].

На основе проведенного анализа был разработан метод передачи данных в системах мгновенного обмена сообщениями с использованием сквозного шифрования.

Опишем компоненты приложения, основанного на предлагаемом решении. Диаграмма компонентов представлена на рис. 1.

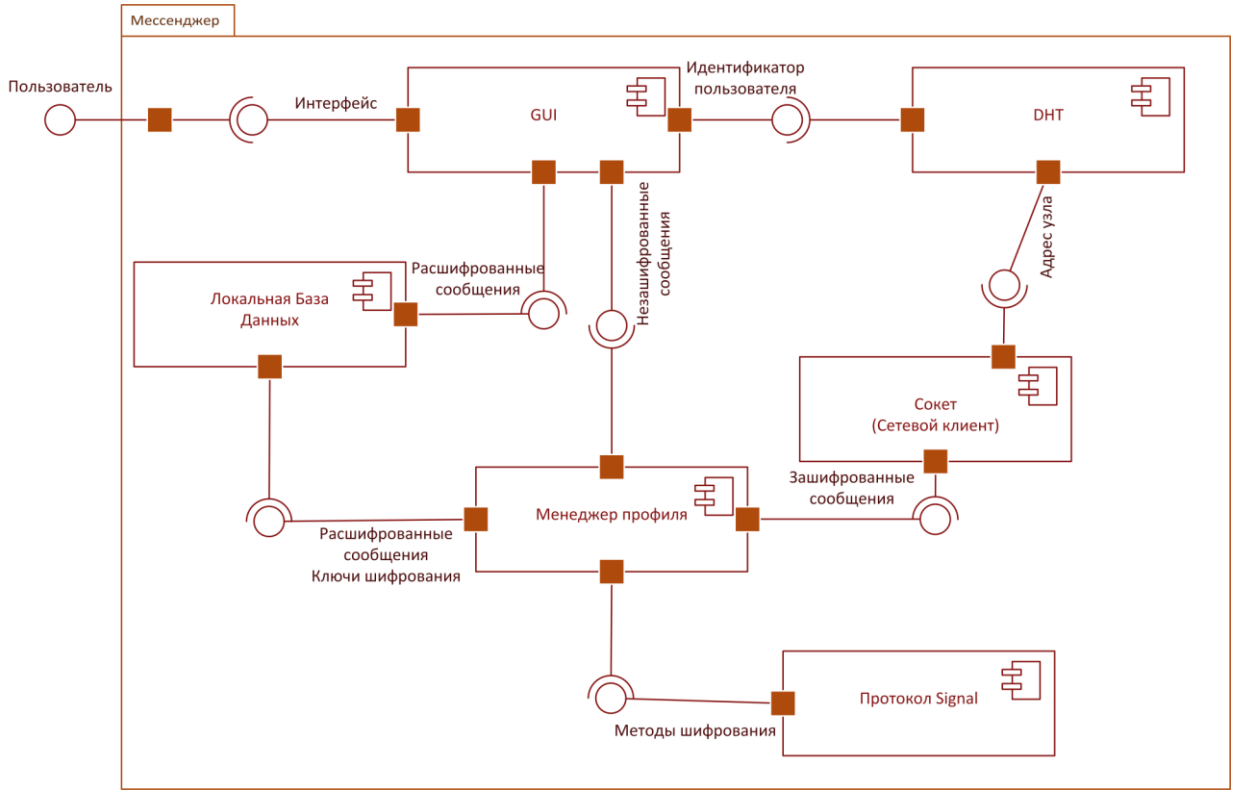

Рис. 1 – UML диаграмма компонентов мессенджера, реализующего предлагаемый метод обмена мгновенными сообщениями.

GUI – графический интерфейс пользователя, получает ввод от пользователя и передает введенные данные соответствующим компонентам системы, после чего отображает результат.

DHT – компонент системы, отвечающий за реализацию распределенной хэш-таблицы. Получает идентификатор пользователя для поиска, после чего проводит поиск по подключенной хэш-таблицы. Передает адрес пользователя сокету.

Сокет – сетевой компонент системы, отвечает за связь с другими пользователями, отправляет и получает зашифрованные сообщения.

Протокол Signal – библиотека протокола. Получает хранилище ключей шифрования, управляет сессиями ключей, расшифровывает и зашифровывает сообщения, а также управляет ключами с помощью расширенного тройного протокола Диффи-Хеллмана (X3DH) [11].

Менеджер профиля – создает и управляет профилем пользователя, хранилищем ключей шифрования и сессий протокола Signal. Получает зашифрованные или незашифрованные сообщения и передает их вместе с хранилищем ключей и сессий протоколу Signal. В ответ получает зашифрованное или расшифрованное сообщение. Зашифрованное передает сокеты, для отправки собеседнику, расшифрованное передает в графический интерфейс пользователя.

Локальная база данных – предоставляет доступ к зашифрованному локальному хранилищу другим компонентам системы. Сохраняет историю сообщений, и данные профиля пользователя, в которые входят хранилище ключей шифрования и сессий протокола Signal.

Приложение с подобной архитектурой подключается к структурированной одноранговой сети, поиск собеседников осуществляется с помощью DHT, что избавляет от уязвимого централизованного сервера. Благодаря использованию протокола шифрования Signal, сообщения устойчивы к большому спектру атак, в том числе MitM. Даже если будет подобран ключ шифрования от одного из сообщений, то все остальные переданные сообщения останутся нескомпрометированными. Благодаря использованию идентификатора пользователя, отличного от номера телефона, решается проблема протокола Signal, при котором можно было связать номер телефона и отправляющего сообщения, из-за чего нарушалось криптографическое свойство отрицания.

Таким образом, был разработан метод обмена мгновенными сообщениями с использованием сочетания лучших способов организации обмена данными и криптографических протоколов обмена мгновенными сообщениями с использованием сквозного шифрования.

Дальнейшими целями проекта является повышение защищенности метаданных передаваемых сообщений, анонимности пользователя в сети,

например, с помощью организации P2P соединения при помощи луковой маршрутизации, организация защищенной групповой переписки, а также реализация защиты DHT от известных атак [12].

Литература (References)

1. Tankovska H. Number of monthly active WhatsApp users worldwide from April 2013 to March 2020. URL: statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/.

2. Schollmeier R. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications // Proceedings – 1st International Conference on Peer-to-Peer Computing, P2P 2001. Institute of Electrical and Electronics Engineers Inc., 2001. P. 101–102.

3. Buford, J.F., H. Yu and E.H. Lua, 2008. Peer-to-peer concepts. P2P Networking and Applications, Morgan Kaufmann, pp: 25-44.

4. Zhang, H., Y. Wen, H. Xie and N. Yu, 2013. Distributed Hash Table - Theory, Platforms and Applications. New York: Springer New York.

5. Jakobsen J., Orlandi C. On the CCA (in) security of MTProto // SPSM 2016 - Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices, co-located with CCS 2016. Association for Computing Machinery, Inc, 2016. P. 113–116.

6. Van Dam D. Analysing the Signal Protocol. URL: ru.nl/publish/pages/769526/z00b_2019_thesis_dion_van_dam_2019_eerder.pdf

7. Cohn-Gordon K., Cremers C., Dowling B., и др. A formal security analysis of the signal messaging protocol // J. Cryptol. Springer, 2020. Vol. 33, № 4. P. 1914–1983.

8. Degabriele J.P., Lehmann A., Paterson K.G., и др. On the joint security of encryption and signature in EMV // Cryptographers' Track at the RSA Conference. Springer, 2012. P. 116–135.

9. Cohn-Gordon, K., C. Cremers and L. Garratt, 2016. On Post-compromise Security. 2016 IEEE 29th Computer Security Foundations Symposium (CSF), IEEE. URL: ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7536374.

10. Hagen C., Weinert C., Sendner C., и др. All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers. 2020.

11. Marlinspike M., Perrin T. The X3DH Key Agreement Protocol. 2016.

12. Urdaneta G., Pierre G., Van Steen M. A survey of DHT security techniques // ACM Comput. Surv. ACM PUB27 New York, NY, USA, 2011. Vol. 43, № 2.