УДК 004.056.55

БЕЗОПАСНАЯ СИСТЕМА ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМИ С ПОВЫШЕННОЙ КОНФИДЕНЦИАЛЬНОСТЬЮ ДАННЫХ

Прыгунов М.И. (Самарский государственный технический университет)
Научный руководитель – кандидат технических наук, доцент Камальдинова З.Ф.
(Самарский государственный технический университет)

Введение. Сейчас в мире представлено много решений так называемых мессенджеров, удобных для всех. Причем одна из самых значимых вещей на которую обращает внимание пользователь при выборе подобного приложения – конфиденциальность. Но так ли хороши системы, которые нам предлагают?

Краткий ответ нет, если изучать вопрос подробнее, то можно узнать, что в большинстве случаев в базе данных информация хранится в открытом для администратора виде. Это дает возможность третьему лицу – администратору, читать личные сообщения пользователей. Получается, что конфиденциальность переписки держится на доверии этому самому администратору. Если человек дорожит своей перепиской, его не устроит подобное обстоятельство.

Администратор может совершать действия для достижения максимальной безопасности данных, но от утечек никто не застрахован. Как пример: год назад была слита база данных пользователей Яндекс Еды [1]. Стоит упомянуть, базы данных в большинстве своем не зашифровываются, это не выгодно для бизнеса, но тем временем та база содержала в себе фамилии, реальные адреса и телефоны, суммы заказов за последние полгода, причем речь не только о постоянных адресах жительства. Фактически по заказам можно отследить все перемещения пользователя по стране, его благосостояние. Для мошенников это очередная возможность. Где бы вы не находились – все будет на карте. Тогда в базе было семь миллионов человек, можно было найти себя и своих близких, в том числе знаменитостей и сотрудников государственных ведомств.

Некоторые мессенджеры громко заявляют о себе сквозным шифрованием. Что же, сквозное шифрование не спасает вас от всех проблем, остается уязвимость: человек по середине, когда кто-то может перехватывать все данные сети в одном узле и подделывать их для сервера. Тем более никто не гарантирует, что сервер сам не будет подделывать ключи и получать доступ к переписке, код у серверов закрытый. Если человек все же доверяет серверу, то существует необходимость проверки совпадения контрольных значений.

Еще одна проблема – анонимность [2], которая уже была частично затронута ранее. Человек, отдавая сервису свой номер телефона, может быть уверен, что при желании по этому номеру можно узнать, где он проживает. Более того, если у злоумышленника есть доступ к данным оператора, с помощью триангуляции можно узнать точное местонахождение человека в текущий момент.

Основная часть. Упомянутые проблемы натолкнули на идею создать максимально конфиденциальный мессенджер, где шифрование и дешифрование будет происходить только на устройствах, а на сервере будет хранится исключительно зашифрованная информация.

У устройств есть общий ключ, с помощью которого происходит расшифровка и шифрование сообщений. Этот ключ никуда не передается и всегда остается на устройствах. Более того, так как весь мир сейчас уже отказался от соединений без шифрования зашифрованное приложением сообщение повторно зашифруется асимметричным шифрованием при передаче через HTTPS. Так что, на уровне сети сообщение будет зашифровано дважды, так достигается гибридная криптографическая схема.

Ключ один, но как начать переписку? Ключ необходимо создать на двух устройствах, для этого генерируется QR-код на одном из них, второй сканирует его и получает ключ к переписке, которая создается на сервере. Если соединяемые устройства обладают технологией

NFC, их достаточно расположить рядом друг с другом для синхронизации ключа. Необходима личная встреча, мы идем на такую жертву ради уверенности в надежности переписки.

Анонимность. В пользу анонимной регистрации приходится отказаться от способов восстановления пароля. Ровно также, как и в хороших блокчейн системах. У пользователя есть логин и пароль, никакой персональной информации. Ответственность за анонимность логина перекладывается полностью на пользователя. Конечно, он может придумать логин вида «ivanov.ivan.2001», тогда уже об анонимности не может быть и речи, а пользоваться подобным приложением ему ни к чему.

Если описывать приложение архитектурно, то можно сказать следующее - алгоритм шифрования может быть выбран любой, в примере далее используется стандарт AES, а чтобы одинаковое сообщение после шифрования принимало разный вид используются разные векторы инициализации [3]. Ключи шифрования, которые хранятся локально на устройствах, будут шифроваться повторно с помощью введенного пользователем пароля доступа, ровно как в хорошем банковском приложении. А в само сообщение закладывается вектор инициализации, зашифрованный текст, псевдоним отправителя, и время отправления.

Код сервера-посредника оставить открытым не составит труда – он будет заниматься только сохранением сообщения в базе данных и его отправкой другим пользователям. Более того, можно провести эксперимент и сделать базу данных открытой - узнать, как долго будет расшифровываться одна случайная переписка. Расшифровав ее, злоумышленнику будет затруднительно понять кому она принадлежит - логин не содержит персональной информации. Более того, как хакеру выбрать ту самую переписку, которая ему интересна для расшифровки?

Выводы. Разработанный продукт позволяет вести безопасную переписку по незащищенному соединению. Безопасность и конфиденциальность переписки не будут зависеть от администратора системы, будут зависеть исключительно от длины ключа и самого пользователя. Чем больше бит занимает ключ, тем дольше будет проходить взлом шифра методом перебора. Со стороны пользователя есть угроза утечки пароля доступа к клиенту, а также не следует генерировать пароль при посторонних лицах, необходимо это учитывать при использовании.

Список использованных источников:

1. Прыгунов М.И. Конфиденциальная система обмена мгновенными сообщениями. В сборнике: Перспективные информационные технологии (ПИТ 2022) [Электронный ресурс]: труды Международной научно-технической конференции / под ред. С.А. Прохорова. – Электрон. текстовые и граф. дан. (12,5 Мбайт). – Самара: Издательство Самарского научного центра РАН, 2022. – С.120-122.
2. Гатчин Ю. А., Коробейников А. Г. Основы криптографических алгоритмов. Учебное пособие. — СПб.: СПбГИТМО (ТУ), 2002.
3. Баричев С. Г., Гончаров В. В., Серов Р. Е. 2.4.2. Стандарт AES. Алгоритм Rijdael // Основы современной криптографии — 3-е изд. — М.: Диалог-МИФИ, 2011. — 176 с.

Прыгунов М.И. (автор) Подпись

Камальдинова З.Ф. (научный руководитель) Подпись