М.И. Прыгунов

КОНФИДЕНЦИАЛЬНАЯ СИСТЕМА ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМИ

(Самарский государственный технический университет)

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 вашу «конфиденциальную» переписку. Получается, что вся ваша конфиденциальность, держится на доверии этому самому администратору. Если вы дорожите своей перепиской, сомневаюсь, что вас устроит такой вариант.

Администратор же, может и совершать много действий для достижения безопасности данных, но от утечек данных никто не застрахован. Как пример: совсем недавно была слита база данных пользователей Яндекс Еды. И как помните, не шло речи ни о каком шифровании, а база тем временем 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 просто раздолье. Где бы вы не находились – все будет на карте. Тогда в базе было 7 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. Да и кто гарантирует что сервер сам не будет подделывать ключи и получать доступ к переписке? Код у серверов закрытый. Наверное, многие пробовали хоть раз создать в приложении секретный чат или совершать звонок с сквозным шифрованием. Так вот если вы убедились, что символы на вашем устройстве совпадают с символами у собеседника – тогда все в порядке и никто не может нарушить обсуждение. Здесь появляется трудность в виде проверки совпадения этих самых символов. Как часто вы обращали внимание на те самые символы?

Еще одна проблема – анонимность. Она была частично упомянута ранее. Даже когда вы отдаете сервису свой номер телефона можете быть уверены, при желании по этому номеру можно узнать, где вы прописаны, а соответственно живете. Более того, если есть доступ к данным оператора, с помощью триангуляции можно узнать точное местонахождение человека в текущий момент.

Такие 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 устройстве. 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.

Что же, 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. Вы правильно поняли - 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 «prygunov.maksim.26052001», 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 по стандарту AES, чтобы одинаковое сообщение после шифрования принимало разный вид используются разные векторы инициализации. Ключи шифрования, которые хранятся локально на устройствах, будут шифроваться повторно с помощью введенного пользователем кода 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, как понять кому она принадлежит, если логин не содержит персональной информации? Как выбрать ту самую переписку, которая интересна злоумышленнику? Тут напрашивается шутка – база данных не может быть слита, если она уже в открытом доступе.

Подводя к завершению, стоит упомянуть, что ответственность за безопасность переписки полностью переложиться на самого пользователя приложения. Никто не сможет гарантировать безопасность, если логин, пароль, код доступа, в конце концов пароль от телефона хранятся на бумаге, пусть и в сейфе.

Литература

1. 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. — С. 30—35. — 176 с.
2. Гатчин Ю. А., Коробейников А. Г. Основы криптографических алгоритмов. Учебное пособие. — СПб.: СПбГИТМО(ТУ), 2002.

А.А. Фирсова, И.В. Константинов

МЕХАНИЗМ ДЛЯ ПРОТИВОДЕЙСТВИЯ DDOS-АТАКАМ, НАПРАВЛЕННЫЙ НА КЛИЕНТОВ ДИФФЕРЕНЦИРОВАННЫХ УСЛУГ

(Поволжский государственный университет
телекоммуникаций и информатики)

Сети с дифференцированным обслуживанием (DiffServ) обеспечивают гарантию качества обслуживания (QoS) методом распределения трафика по фиксированному числу ранее существовавших классов. Атаки типа DoS/DDoS на клиентов DiffServ становятся все более целенаправленными и требуют меньшей пропускной способности, чем текущие атаки, из-за ограничений пропускной способности для каждого клиента и класса, которые должны быть наложены для обеспечения гарантий качества обслуживания. В этой статье представлена техника отражения DDoS-атаки на клиенте DiffServ посредством динамической модификации заголовков пакетов. Этот механизм позволяет сети DiffServ отличать легитимный трафик от вредоносного трафика, но не требует криптографической обработки для каждого пакета и не увеличивает размер пакета.

Дифференцированный сервис обеспечивает QoS без сохранения информации о состоянии каждого потока в основных маршрутизаторах. Пограничные маршрутизаторы контролируют трафик, входящий в сеть, классифицируя и обрабатывая его, чтобы он соответствовал определенному агрегату поведения на основе соглашения об уровне обслуживания (SLA) между источником и поставщиком DiffServ. Основные маршрутизаторы не отслеживают состояние отдельных потоков. Они несут ответственность только за пересылку на основе маркировки, присвоенной каждому пакету при его поступлении в сеть.

DDoS-атаки пытаются искусственно истощить ресурсы поставщика услуг, такие как пропускная способность, память или циклы процессора. Большинство DDoS-атак основаны на одной и той же концепции. Злоумышленник компрометирует группу нецелевых хостов и заставляет их отправлять поток трафика на целевую систему. Этот лавинный трафик потребляет полосу пропускания на канале к цели, вызывая переполнение очереди на канале. Адреса источников в заголовках пакетов обычно изменяются, чтобы предотвратить обнаружение скомпрометированных узлов.