УДК 004.223.2

СОЗДАНИЕ СХЕМЫ ЗАЩИЩЁННОЙ ПЕРЕДАЧИ СООБЩЕНИЙ МЕЖДУ ПОЛЬЗОВАТЕЛЯМИ

В.В. ПЕТЮКЕВИЧ
(Представлено: канд. физ.-мат. наук, доц. Д.Ф. ПАСТУХОВ)

Рассматривается проектирование схемы защищённой передачи данных между пользователями по схеме peer-to-peer, также вопросы защиты этих данных. Проведён анализ технологий, наиболее подходящих, для разработки данной схемы.

Введение. Некоторые средства передачи информации между пользователями, такие как Viber и Telegram, используют шифрование сообщений, однако осуществляют передачу сообщений через собственные сервера. Таким образом получается, что все сообщения пользователей могут храниться на сервере и, впоследствии, быть переданными кому-либо.

Эту проблему можно решить, используя peer-to-peer соединение.

Peer-to-peer сеть – оверлейная компьютерная сеть, основанная на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются пиры [1].

Преимущества, получаемые при использовании peer-to-peer:

1. Защита от утечки данных со стороны сервера;
2. Снижение нагрузки на сервер приложения, т. к. сервер перестанет участвовать в процессе пересылки сообщений.

Существующие решения.

Ни одно из популярных средств обмена сообщениями не использует защиту сообщений на максимально возможном уровне. Viber и Telegram используют end-to-end шифрование, но их общая проблема – это контроль всего процесса передачи сообщений серверами этих сервисов.

Ent-to-end шифрование – способ передачи данных, в котором только пользователи, участвующие в общении, имеют доступ к сообщениям. Таким образом, использование сквозного шифрования не позволяет получить доступ к криптографическим ключам со стороны третьих лиц [2].

Тема совмещения end-to-end шифрования и peer-to-peer соединений раскрыта недостаточно хорошо. В интернете была найдена только одна статья на английском языке. Но в данной статье были рассмотрены только теоретические вопросы без рассмотрения вариантов используемых технологий.

Средства решения задачи.

В данной статье рассмотрен только случай передачи текстовых данных. Однако, используемые в данной схеме технологии можно применить и для передачи данных других видов.

End-to-end шифрование в peer-to-peer сети позволит избежать проблему перехвата пересылаемых данных. Так же, данное приложение должно работать в браузере, чтобы пользователю не приходилось ничего устанавливать.

В связи с требованиями, для установки peer-to-peer соединения между клиентами используется WebRTC:

WebRTC – проект с открытым исходным кодом, предназначенный для организации передачи потоковых данных между браузерами или другими поддерживающими его приложениями по технологии peer-to-peer [3].

На уровне API технология стандартизируется консорциумом W3C, а на протокольном уровне — сообществом IETF. Его включение в рекомендации W3C поддерживается Google Chrome (и других на его основе), Mozilla и Opera.

Преимущества технологии:

1. Проведение конференции в браузере значительно упрощает процесс проведения конференции – пользователю не нужно устанавливать для этого отдельные приложения;
2. Используемые кодеки обеспечивают хорошее качество связи;
3. Возможность реализации любых элементов интерфейса средствами HTML5 и JavaScript;
4. Открытый исходный код даёт больше возможностей для использования.

Недостатки технологии:

Технология определяет только общий стандарт передачи данных (видео и звука), но отдельные решения разных браузеров относительно адресации абонентов и прочих управляющих процессов не сов-

местимы между собой. Поэтому даже звонки между парой различных браузеров представляют отдельную сложность.

Для end-to-end шифрования применяется протокол Диффи–Хеллмана:

Протокол Диффи–Хеллмана – криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования [4].

Описание схемы передачи сообщения**:**

1. При авторизации клиенты генерируют, по протоколу Диффи-Хеллмана, свою пару открытый/закрытый ключ и отправляют открытый ключ на сервер;
2. Перед отправкой сообщений, клиенты через сервер получают открытые ключи друг друга и обмениваются сообщениями для установки peer-to-peer соединения через WebRTC. Для снижения нагрузки на сервер, сообщения установки peer-to-peer соединения передаются через протокол WebSocket;
3. В результате получения открытых ключей друг друга, клиенты могут сгенерировать общий ключ по протоколу Диффи-Хеллмана;
4. После установки peer-to-peer соединения, клиенты могут обмениваться зашифрованными общим ключом сообщениями.

Алгоритмы, использующиеся в данной схеме:

1. Для создания пары открытый/закрытый ключ используется протокол Диффи-Хеллмана;
2. Для генерации закрытого ключа используется алгоритм HMAC-SHA256 с размером блока 64 бит. Алгоритмом HMAC-SHA256 хэшируется имя пользователя и случайное число. Сделанно это для того, чтобы при каждой новой сессии ключ получался разным;
3. Для шифрования сообщений используется алгоритм AES с длиной ключа 256 бит и размером блока 64 бит. В качестве ключа для шифрования/дешифрования сообщений используется общий ключ двух пользователей, который был получен по протоколу Диффи-Хеллмана.

Установка Peer-to-Peer соединения между двумя клиентами:

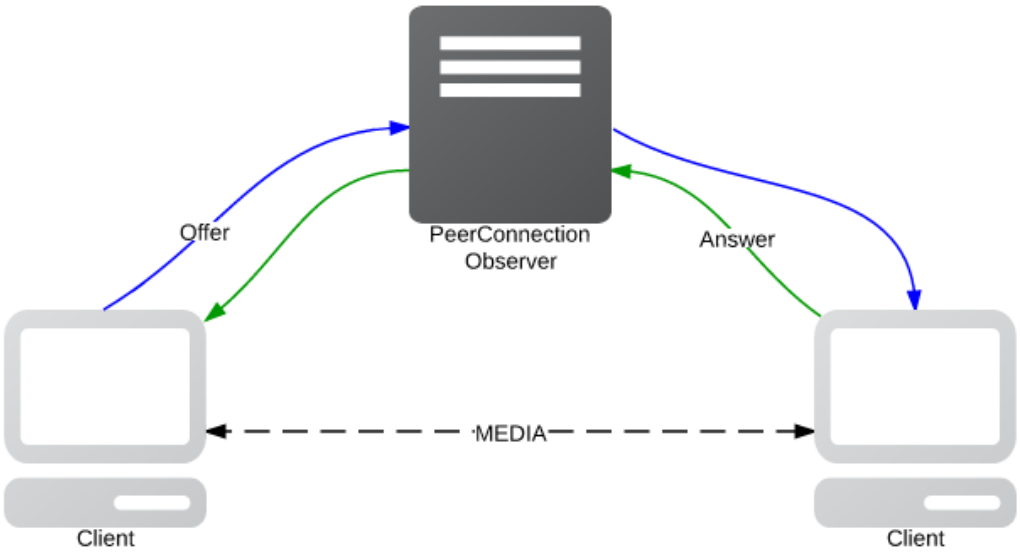

Рисунок. – Схема peer-to-peer соединения между двумя клиентами

Упрощенная схема соединения между двумя клиентами:

1. Первый клиент отправляет так называемый Offer второму клиенту через сервер;
2. Второй клиент отправляет через сервер ответ первому клиенту;
3. Устанавливается peer-to-peer соединение между клиентами.

Таблица 1. – Замеры скорости шифрования реализации AES на языке JavaScript

Количество символов	Время, с
200	0,3
500	0,6
1000	1

Для быстрой передачи сообщений на сервер используется протокол WebSocket. WebSocket – протокол полнодуплексной связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером в режиме реального времени [5]. В сравнении с HTTP, WebSocket передаёт намного меньше служебной информации с каждым запросом.

Заключение. В ходе данного исследования был спроектирована схема защищённой передачи данных между пользователями с использованием end-to-end шифрования в peer-to-peer сети. End-to-end шифрование было реализовано через протокол Диффи-Хеллмана с использованием алгоритмов HMAC-SHA256 и AES. Для установки peer-to-peer соединения в браузере был использован WebRTC. Следует отметить, что разработанная схема оставляет возможность для доработки и введения дополнительных средств защиты.

ЛИТЕРАТУРА

1. Материал из Википедии – свободной энциклопедии [Электронный ресурс] // Одноранговая сеть. – Режим доступа: https://ru.wikipedia.org/wiki/Одноранговая_сеть. – Дата доступа: 20.09.2018.
2. Бутакова, Н.Г. Криптографическая защита информации : учеб. пособие для вузов / Н.Г. Бутакова, В.А. Семененко, Н.В. Федоров. – М. : Изд-во МГИУ, 2011. – С 91–102.
3. Материал из Википедии – свободной энциклопедии [Электронный ресурс] // WebRTC. – Режим доступа: https://ru.wikipedia.org/wiki/WebRTC. – Дата доступа: 20.09.2018.
4. Материал из Википедии – свободной энциклопедии [Электронный ресурс] // Протокол Диффи-Хеллмана. – Режим доступа: https://ru.wikipedia.org/wiki/ Протокол_Диффи_—_Хеллмана. – Дата доступа: 20.09.2018.
5. Материал из Википедии – свободной энциклопедии [Электронный ресурс] // WebSocket. – Режим доступа: https://ru.wikipedia.org/wiki/WebSocket. – Дата доступа: 20.09.2018.