УДК 004.057.4

РАЗРАБОТКА АРХИТЕКТУРЫ РЕШЕНИЯ, ПОЗВОЛЯЮЩЕГО СОХРАНЯТЬ ВИДЕОЗВОНКИ, СОВЕРШЁННЫЕ С ПОМОЩЬЮ WebRTC

А. Д. Дёмин (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург)

Научный руководитель: Д. А. Зубок (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург)

Имеется система, работающая под управлением операционных систем Android и iOS, которая позволяет пользователям совершать видеозвонки. Данная система работает с использованием WebRTC – это проект с открытым исходным кодом, предназначенный для организации передачи потоковых данных между поддерживающими его приложениями (в частности, через браузеры, также имеется API для Android и iOS) методом точка-точка. Необходимо реализовать возможность сохранения медиатрафика (аудио и видео), поскольку правоохранительные органы различных стран могут требовать предоставления доступа к этой информации в случаях, установленных в законах соответствующих стран. Реализация такой доработки в системе имеет следующие технические сложности:

- соединение между абонентами может иметь вид точка-точка, что не позволяет получить доступ трафику между абонентами;
- весь медиатрафик между абонентами передаётся зашифрованным;
- для проведения данной доработки необходимо сформировать понимание того, какая информация является достаточной для преобразования сохранённого медиатрафика в воспроизводимые аудио- и видеоформаты;
- необходимо провести доработку так, чтобы минимально затронуть уже существующую архитектуру системы;
- после проведения доработки необходимо обосновать безопасность пользовательских данных от несанкционированного доступа к ним злоумышленников.

Целью работы является разработка архитектуры решения, которая позволит сохранять видеозвонки, произведённые с помощью WebRTC, с минимальными доработками в существующей системе. Для этого были решены следующие задачи:

- было предложено решение о проксировании трафика между пользователями, для того чтобы иметь к нему доступ и описано, как реализовать данное решение;
- было проведено изучение механизмов шифрования, использующихся в WebRTC, их методов формирования и передачи ключей, возможность получения ключей к медиапотокам, а также возможности замены используемых алгоритмов шифрования другими; по результатам этого исследования был выбран метод шифрования медиапотока, который позволит на сервере системы получить доступ к проходящему трафику медиапотоков;
- для выбранного метода шифрования было теоретически обосновано, почему при возможности доступа из системы к пользовательскому медиатрафику уровень защищённости данных пользователей от злоумышленников не стал меньше;
- было рассмотрено, какие данные необходимо сохранить для возможности преобразования сохранённого медиатрафика в воспроизводимые аудио- и видеоформаты;

На основе информации, полученной в ходе решения задач работы, была разработана архитектура системы, решающая все технические сложности, обозначенные выше, и которая будет применяться при дальнейшем проведении реализации доработки в системе.

Литература:

1. draft-ietf-rtcweb-security-arch-18 - WebRTC Security Architecture. [Электронный ресурс]. URL: https://tools.ietf.org/html/draft-ietf-rtcweb-security-arch-18
2. RFC 3261 - SIP: Session Initiation Protocol. [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc3261 (Дата обращения: 16.02.2019)
3. RFC 4568 - Session Description Protocol (SDP) Security Descriptions for Media Streams. [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc4568 (Дата обращения: 18.02.2019)
4. RFC 5766 - Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN) [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc5766 (Дата обращения: 18.02.2019)
5. Signaling and video calling. [Электронный ресурс]. URL: https://developer.mozilla.org/en-US/docs/Web/API/WebRTC_API/Signaling_and_video_calling (Дата обращения: 18.02.2019)
6. Support of SDES in WebRTC. [Электронный ресурс]. URL: https://tools.ietf.org/id/draft-ohlsson-rtcweb-sdes-support-00.html (Дата обращения: 18.02.2019)
7. WebRTC 1.0: Real-time Communication Between Browsers. [Электронный ресурс]. URL: https://w3c.github.io/webrtc-pc/ (Дата обращения: 17.02.2019)