РЕАЛИЗАЦИЯ SSL СЕРТИФИКАТА В МЕССЕНДЖЕРЕ

Карпов Г.И.

В наши дни сеть Интернет объединяет более сотни миллионов людей по всему миру. Большую часть информации мы получают благодаря различным информационным ресурсам, мессенджерам и многому другому. Каждый день сотни миллионов людей используют различные сайты для передачи и поиска информации. Основное человеческое общение переместилось в сеть Интернет, что не могло сказаться на личной безопасности

каждого. Для сохранения и защиты данных в любых сервисах используются различные методы и инструменты, которые с большой долей вероятности помогают нам доверить информацию о себе им и защититься от будущих хакерских атак. Всем известно, что сертификаты обеспечивают безопасное соединение клиента с сервером, в данной курсовой работе демонстрируется подход, который был реализован как программное обеспечение шифрования на сокетах в сетях с помощью SSL-сертификата, использующего отечественный метод симметрического шифрования [1, с. 3–18].

Для реализации клиент-серверного приложения с SSL сертификатом необходим сервер, который генерирует секрет (большое число 256 бит) с помощь отдельной написанной функции, которая в последствии будет использоваться для шифра и делит его на n частей (n – частей зависит от количества клиентов в чате), и отправляет части этого секрета, разделенного по схеме Асмута-Блума клиентам. Первый пользователь, который подключается к серверу задает число m клиентов наличие которых необходимо для восстановления секрета, а также для последующей проверки количества клиентов на сервере, то есть, если m не равно числу клиентов на сервере, то соединение обрывается автоматически.

Далее рассмотрим взаимодействие подключение клиентов к серверу. Клиент посылает серверу запрос на присоединение. Сервер отправляет клиенту свой сертификат. Далее клиент его проверяет на подлинность. Если проверка прошла успешно, то взаимодействие продолжается, если нет, то соединение обрывается автоматически. Рассмотрим дальнейшую работу программы при успешной проверке. Клиент отправляет серверу служебную информацию об успешности проверки и сервер в ответ отправляет запрос на долю секрета, в последствии которую будет проверять на подлинность. При успешной проверке секрета клиент генерирует параметры шифра и отправляет серверу свой открытый ключ. После того как сервер получил открытый ключ пользователя он с его помощью шифрует новый ключ и синхропосылку для общения между клиентами и отправляет шифрограмму конкретному клиенту.

Подтверждение подлинности клиентов и сервера произошло, и далее рассмотрим общение между клиентами. На этапе подключения к серверу клиент в случайном порядке выбирает шифр для связи с другими клиентами (Магма, Магма с гаммированием, Магма с гаммированием и обратной связью, кузнечик). С помощью выбранного шифра он шифрует отправленные сообщения и на сервер приходят зашифрованные данные. Далее сервер рассылает их всем клиентам (групповой чат). Получив зашифрованные сообщения, клиенты выбирают по метаданным каким шифром их расшифровать. Таким образом, происходит подключение и обмен сообщениями между клиентами.

Литература

1. Ivan R, Melinda R. Bulletproof SSL and TLS. London, 2015. 530 p.