УДК 004.056.53

ШИФРОВАНИЕ И ПЕРЕСЫЛКА СООБЩЕНИЙ БЕЗ СЕРВЕРА

Р.В. Елисеев, муниципальное бюджетное общеобразовательное учреждение лицей при ТПУ, Томск.

Научный руководитель - аспирант В.Е. Воротов, федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Томский политехнический университет», г. Томск

Защита данных с помощью криптографического преобразования является эффективным решением проблемы их безопасности. Зашифрованные данные доступны лишь тем, кто знает, как их расшифровать, то есть тем, кто обладает соответствующим ключом шифрования, но в современном мире при пересылке сообщений нельзя быть полностью уверенным в целостности пересылаемой информации и в получении ее конечным пользователем без посредников.

Целью проекта является разработать комплекс мер, позволяющих совершать гарантированно безопасный обмен сообщениями в глобальной сети.

При реализации данного проекта были выявлены следующие проблемы:

1) Невозможность установления соединения между двумя компьютерами с «серыми» ip адресами, если обоим клиентам известны лишь взаимные адреса.
2) Возможность активной MITM атаки ввиду множества узлов в соединении двух клиентов.

Стоит отметить, что актуальным решением данной проблемы является использование сертификационных центров и серверов. Но подобное решение основано на безусловном доверии центрам сертификации и держателям серверов.

Также возможным решением может служить blockchain, но подключения к конкретной сети большого количества устройств, что довольно трудно обеспечить.

Установление соединения компьютер-компьютер в глобальной сети

В данный момент широко используемым интернет-протоколом является ipv4, те адрес устройства занимает 4 байта(~4млрд уникальных адресов) , в то время как на 2018 год количество устройств, подключенных к интернету оценивалось как 22млрд. Это в свою очередь влечет так называемые «серые» ip адреса, те у нескольких компьютеров могут быть одни и те же ip адреса в глобальной сети. И это не вызывает проблем, если компьютер устанавливает соединение с сервером, у которого «белый» ip адрес, ведь подключается он по определенному порту, те маршрутизатор понимает на какой именно компьютер направить ответ от сервера. Но нельзя установить соединение с компьютером с «серым» ip адресом, у него не открыт порт на прослушку. А если учесть, что задача стоит так, что между клиентами нет защищенного канала связи, то они не могу обменяться взаимными ip адресами и портами, тогда решением может служить любой компьютер с «белым» ip адресом, которому мы доверяем. Данный компьютер будет служить для сообщения клиентам их взаимных ip адресов и портов. При этом стоит понимать, что требования к производительности компьютера крайне малы. Так, в ходе тестирования реализованная программа проверялась на компьютере с устаревшим процессором Intel Core 2 Duo E6300, 1гб ОЗУ и операционной системой, установленной на флэш-накопитель и указанная сборка справилась с поставленной задачей-помогла установить соединение более чем 10-ти

клиентам. Также, в целях экономия места и большего удешевления проводилось тестирование на Raspberry pi, которая также прекрасно справилась с задачей.

Таким образом было реализовано решение, позволяющее установить соединение между двумя компьютерами в глобальной сети без больших затрат на выделенный сервер.

Обеспечение целостности и конфиденциальности при обмене сообщениями

Как было описано ранее ввиду того, что обмен сообщениями ведется в глобальной сети, невозможно гарантировать отсутствие возможности активной MITM атаки, которая не позволяет использовать ассиметричный алгоритм шифрования в чистом виде. Тогда решением служит наш компьютер, публичный ключ которого известен заранее всем участникам. Тогда, следуя следующему алгоритму клиенты смогут установить соединение друг с другом:

1) Алиса и Боб шифруют свои открытые ключи меньшей длины, чем у сервера(например у сервера 2048 бит, а у клиентов по 1024 бита) открытым ключом общего компьютера
2) Компьютер отправляет Алисе ip адрес Боба и открытые ключи Алисы и Боба(ключ Алисы отправляется для защиты от активной MITM атаки на первом этапе). Бобу аналогично.
3) Алиса и Боб заводят общий ключ симметричного шифрования(например AES)

Таким образом у обоих клиентов есть общий ключ симметричного шифрования, что гарантирует конфиденциальность и целостность информации без привязки нашему компьютеру и какому бы то ни было конкретному каналу связи. Те теперь обмен можно вести через любой удобный канал связи при этом без ограничения размеров файлов.