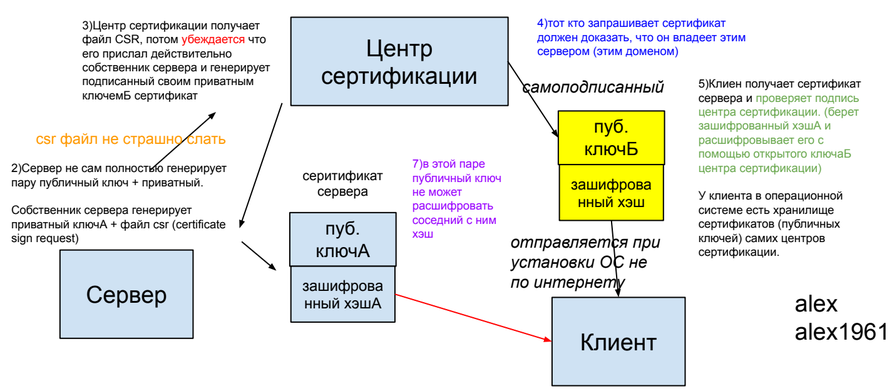


1)Чтобы начать общение клиенту и серверу, надо чтобы сервер сгенерировал публичный и приватный ключ и отправил публичный ключ клиенту.

Чтобы не было атаки “Человек посередине” клиент должен иметь возможность проверить, что полученный публичный ключ принадлежит серверу.

Чтобы этого достичь сервер присылает не просто публичный ключ, а сертификат. Это файл в котором есть публичный ключ + подпись центра сертификации.

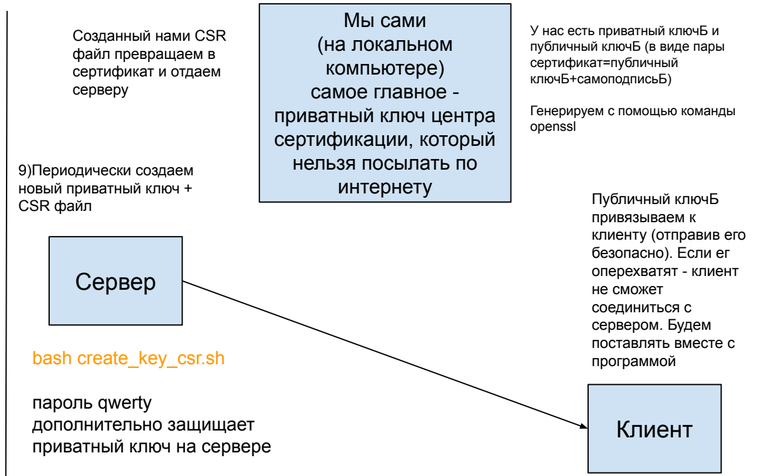
Подпись это зашифрованный хэш данных с помощью приватного ключа центра сертификации.

9)злоумышленник захочет поменять публичный ключА в этой паре

в случае подмены после расшифровки подписи хэшА не совпадет с хэшем, который можно сгенерить с помощью публичного ключаА

6)самоподписанный сертификат - тот кто выпускает сертификат своим же приватным ключом его подписывает (шифрует), а расшифровать можно лежащим рядом публичным ключом

8)мы получим сам хэшА и проверим, что этот хэш соответствует публичному ключуА от сервера (клиент сам вычисляет хэш по публичному ключуА и сравнивает 2 хэша)



в дальнейшем
1.при получении нового клиента - мы просто кладем рядом с ним сертификатБ (содержащий публичный ключБ центра сертификации). И всем клиентам его кладем, и постараемся его не менять

2.если мы поменяем на сервере приватный ключ, то все в порядке - на клиенте не надо ничего менять

cd /mnt/c/Users/Alex/Downloads/im/vi/superchat/client_v20
или shift+правая кнопка мыши
openssl = первая проверка, что openssl не неизвестная команда
пароль к приватному ключу центра сертификации asdf

сейчас есть внутренний сервер, который нужен, чтобы 2-ая копия с тем же unidque key вообще не запустилась. Если бы она даже запустилась - то к серверу она все равно бы не подключилась (был бы тот же эффект, что с другого компьютера - было бы просто написано connecting)

внутренний сервер обращается по ip адресу 127.0.0.1 (совсем в интернет не выходит)

текущий ip адрес компьютера называют локалхостом

и если мы запустим на ip адресе маршрутазотора сервер

ipconfig
192.168.88.230 - мой адрес компьютера в локальной сети под домашним роутером
(это локалхост)

192.168.88.231 - адрес 2 компьютера в локальной сети под домашним роутером

192.168.88.1 (основной шлюз - адрес моего роутера под самим собой)

80.71.252.248
адрес на столбе

сервера, запущенные на 127.0.0.1 видны только внутри компьютера и могут быть использованы для межпрограммного взаимодействия

мы запускаемся на 127.0.0.1 и один из клиентов хэширует с помощью sha1 юник ключ и отправляет его на фиксированные 10 портов внутри компьютера, где могут жить другие клиенты. И если хэш отправленный совпадет с чьим-нибудь хэшом, то в ответ он получит deny, а иначе от всех accept. Если не шифровать внутреннее кольцо, то можно подсмотреть хэш с помощью wireshark и подменить его любым набором чисел той же длины - тогда они не совпадут, придет accept и мы запустим 2клиента в зависшем состоянии. Чтобы шифрануть - мы должны хранить приватный ключ рядом с клиентом в зашифрованном виде каким-то паролем. Но если пароль подобрать - то будет взлом. Сам пароль хранится в коде

ip.dst == 146.59.154.83
ip.dst == 146.59.154.83 or ip.src == 146.59.154.83
tcp.port == 50171