Протокол SSH

Александр Романов

October 2024

1 Актуальность

В современном мире компьютеры являются неотъемлимой частью работы и повседневной жизни. Люди используют их для большого спектра задач. Начиная с потребления простого медиа, такого как текст или видео, заканчивая компиляцией сложнейших программ и расчётом больших языковых моделей. Однако с развитием рынка высокопроизводительных комплектующих становится видно, что производительность растёт намного медленнее цены. Начиная с некоторой точки прирост производительности на 10% может увеличить стоимость компьютера на 50% и больше. Это сильно усложняет процесс предоставления вычислительной мощности многим людям сразу. Также крайне важной задачей современного мира является управление многими компьютерами сразу (будь то администрирование серверного центра или домашнего роутера). Получать физический доступ к каждому из устройств может быть сложно или вовсе невозможно. Во всех этих случая на выручку приходит протокол SSH, позволяющий дистанционно получать безопасный доступ к любому компьютеру в вашей сети. Данный протокол позволяет давать нескольким людям доступ к одному высокопроизводительному компьютеру для одновременной удалённой работы. Об этом протоколе далее и пойдёт речь.

2 Что такое SSH

SSH или Secure Shell - это сетевой протокол для безопасной коммуникации между клиентом и сервером по небезопасной сети. Чаще всего этот протокол используется для удалённого управления серверами и передачи данных. Также SSH можно использовать для установления безопасных тунелей для других протоколов. В частности, автор данного эссе часто использует подобные тунели для подключения к закрытым портам удалённых серверов по HTTPS (HyperText Transfer Protocol Secure). SSH шифрует передаваемую информацию, защищая её от подслушиваний и вмешательств.

3 Историческая справка

Вопрос дистанционного управления и передачи информации возникли задолго до появления SSH. В частности для администрирования удалённых серверов использовались такие протоколы как Telnet и rlogin. Они, однако, пересылали информацию в виде текста и были уязвимы ко всем видам атак. В 1995 году эти уязвимости привели к сбросу пароля в сети Технологического университета Хельсинки, где в это время находился исследователь Тату Юлёнен. Данное событие подтолкнуло исследователя к разработке первой версии протокола SSH-1. Этот протокол быстро обрёл популярность, несколько разных реализаций и стал известен миру как SSH.

4 Принцип работы SSH соединения

SSH соединение устанавливается в нескольких ключевых шагов, каждый из которых направлен на установление защищённого канала связи. Эти шаги это: Запрос соединения, обмен версиями, обмен ключами, выбор алгоритма обмена ключами, обмен ключами, вычисление ключа сессии и аутентификация. Мы разберём каждый из этих этапов.

4.1 Запрос соединения

SSH клиент запрашивает соединение с сервером, отправляя запрос на специально выделенный TCP (Transfer Control Protocol) порт. Данный порт выбирается администратором сервера и может быть выбран произвольно. Порт по умолчанию для SSH подключения - это порт 22.

4.2 Обмен версиями

На этом этапе сервер отвечает клиенту, отправляя ему свою версию SSH протокола. И клиент, и сервер должны убедиться, что их версии протоколов совместимы и они могут продолжить процесс установки соединения, будучи уверенными, что они будут понимать сообщения друг-друга.

4.3 Выбор алгоритма обмена ключами

Существуют разные алгоритмы обмена ключами. Перед генерацией ключей клиент и сервер должны договориться о том, какой из алгоритмов они будут использовать. Наиболее популярными алгоритмами обмена ключами являются:

- Протокол Диффи-Хеллмана - криптографический протокол, позволяющий нескольким

устройствам получить общий тайный ключ, общаясь через незащищённый канал. Принцип состоит в генерации у каждого из устройств пары из публичного и приватного ключа, обмены публичными ключами через незащищённое соединение и последующего вычисления секрета, используя свой приватный ключ и публичный ключ собеседника

- Протокол Диффи-Хеллмана на элепьических кривых (ECDH) - вариация протокола

Диффи-Хеллмана с использование элиптической криптографии. Полагаясь на сложность дискретного логарифмирования на эллиптической кривой, данный алгоритм позволяет быстрее генерировать ключи меньшей длинны без потери защищённости.

4.4 Вычисление ключа сессии

После обмены ключами по алгоритму, на который договорились устройства все стороны могут использовать эти ключи для генерации ключа сессии. Именно этот ключ будет использоваться для шифрования всех данных, передаваемых по протоколу. Начиная с этого момента подключение можно считать защищённым.

4.5 Аутентификация

Наконец, после установления защищённого подключения клиент может пройти аутентификацию на сервере. Данный процесс может происходить разными способами, которые может настроить администратор сервера:

- Использование пароля. В данном методе клиент пересылает имя пользователя и пароль на

сервер. Несмотря на простоту, этот способ аутентификации не рекомендуется использовать из-за меньшей безопасности.

- Аутентификация при помощи публичного ключа клиента. В данном методе снова используется

ассиметричное шифрование. Для его работы сервер хранит публичный ключ клиент и проверяет подключающегося клиента на наличее соответсвующего приватного ключа. После успеха аутентификации SSH подключение считается установленным и устройства могут занятся передачей полезной нагрузки.