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.

5 Структура протокола SSH

SSH состоит из трёх главных слоёв, каждый из которых отвечает за разные аспекты безопасной коммуникации.

5.1 Транспортный уровень На этом уровне обеспечивается безопасное, зашифрованное

подключение между клиентом и сервером, как было описано выше (см. Раздел 4).

5.2 Уровень пользовательского подключения Данный уровень отвечает за

аутентификацию пользователя, определяя его личность и позволяя подключение только разрешённым клиентам.

5.3 Уровень подключений Данный уровень позволяет иметь несколько логических

каналов, работающих через единственное SSH соединение. Каждый из таких каналов может использоваться для разных целей, таких как доступ к командной строке, передача файлов, портов TCP или передача графической информации таких технологий как X11 и Wayland. Данная способность протокола SSH позволяет использовать разные части сервера без необходимости создавать новые соединения на каждую из задач.

6 Криптография в SSH

SSH использует много разных аспектов современной криптографии для создания безопасного подключения: + Симметричное шифрование Симметричная криптография используется для шифрования передаваемых данных после установки соединения. Наиболее распространёнными алгоритмами симметричного шифрования являются: - AES (Advanced Encription Standard) является стандартом шифрования, принятым правительством США - Blowfish - алгоритм шифрования с ключём переменной длинны, разработанный Брюсам Шнайнером в 1993 году. Часто этот алгоритм предоставляет лучшую производительность чем AES - 3DES это устаревший алгоритм шифрования, который, тем не менее, всё ещё используется на более старых системах.

1. Ассимитричное шифрование Ассиметричная криптография используется для установки соединения и аутентификации пользователя. Наиболее распространёнными алгоритмами явяются: - RSA (от фамилий Rivest-Shamir-Adleman) - это широкораспространённый алгоритм, основывающийся на сложности вычисения больших простых чисел. - DSA (Алгоритм Цифровой Подписи). Этот алгоритм чаще всего используется для создания цифровых подписей, но также применим к обмену ключами. - ECSDA (Алгоритм цифровой подписи на эллиптических кривых) - алгоритм, позволяющий уменьшить размер ключей без потери в безопасности.
2. Хэш-функции Хэш-функции используются как во многих алгоритмах шифрования, используемых SSH. Позволяя обеспечить как безопасность передаваемых данных, так и безопасность самого подключения. Наиболее распространёнными хэш-функциями являются: - MD4 - один из наиболее устаревших хэш функций. Не рекомендована к использованию. - SHA-1 - алгоритм, генерирующий для значения произвольной длины (вплоть до $2^{64} - 1$ бит) значения хэша длины 160-бит. Основывается на тех же принципах, что и MD4. - SHA-256 - Наиболее современная и надёжная хэш-функция. Именно эта функция является предпочтительной заменой устаревшего SHA-1

7 Тунелирование

Как было оговорено выше, протокол SSH позволяет открывать несколько каналов передачи информации через единственное SSH соединение. Перечислим наиболее распространённые применения данной возможности протокола: + Перенаправление портов SSH-тунель позволяет безопасно перенаправлять порты одного устройства на другие порты второго устройства. Перенаправление портов позволяет подключаться к сервисам одного сервера через устройство в другой, незащищённой сети без необходимости открывать этот порт для доступа из незащищённой сети. Автор данной статьи использует перенаправление портов через SSH для подключения к своим web-сервисам, расположенным на его сервере в другом городе.

1. Перенаправление X11 SSH также широко используется для перенаправления данных с графического сервера X11 или Wayland. Это позволяет многим пользователям со слабыми устройствами

подключаться к одному высокопроизводительному серверу для работы над такими сложными графическими приложениям как обработка фото и видео файлов.

8 Рекомендации к использованию

Перечислим некоторые рекомендации по использованию протокола SSH на своих устройствах и серверах: + Запрет аутентификации по паролю Рекомендуется отключить возможность подключения с использованием имени пользователя и пароля. Данные метод подключения считается крайне небезопасный и подлежит атакам.

1. Регулярное обновление ключей SSH ключи обеспечивают высокий уровень безопасности, но для наибольшей защищенности даже их необходимо регулярно менять.
2. Использование современных алгоритмов Для повышения безопасности подключения рекомендуется использовать наиболее современный хэш-функции (Например SHA-256).
3. Просмотр журнала Регулярное наблюдение за журналом вашего сервера поможет заранее заметить подозрительную активность и предотвратить потенциальные атаки.
4. Замена SSH порта Рекомендуется сразу заменять порт, используемый вашим устройством для SSH соединений. Значение порта по умолчанию 22 и злоумышленники знают этот факт, концентрируя свои атаки на этот порт.
5. Настройки файрвола Для обеспечения дополнительной безопасности можно ограничить набор IP-адресов, которым разрешено подключаться к вашему серверу по SSH.

9 Заключение В современном мире протокол SSH является неотъемлимой частью

передачи информации. Сферы его применения варьируются от использования компьютерных игр на удалённых устройствах и рабочих задач, таких как удалённая разработка и компиляция приватного кода на закрытых от внешней сети серверах, до таких требовательных к вычислетельной мощности задач как обработка и создание графического фото и видео контента (В том числе 3D). Многослойная структура этого алгоритма и утилизация им современных криптографических механизмов в группе с настраиваемой аутентификацией делаю SSH поистине незаменимым во всех отраслях технологической сферы. Понимая принцип работы этого протокола и используя рекомендации пользователи могут значительно увеличить безопасность своих подключений в всё более цифровом мире. SSH находится в активной разработке как большими компаниями, так и сообществами добровольцев и адаптируется к новейшим открытиям в мире криптографии. Всё это обеспечивает неустаревающую безопасность.

Библиография

[1] Tatu Ylonen, «ANNOUNCEMENT: Ssh (Secure Shell) Remote Login Program». 12 июль 1995 г.

[2] Tatu Ylonen; C. Lonvick, «The Secure Shell (SSH) Protocol Architecture». [Онлайн]. Доступно на: https://datatracker.ietf.org/doc/html/rfc4251

[3] Tatu Ylonen; C. Lonvick, «The Secure Shell (SSH) Authentification Protocol». [Онлайн]. Доступно на: https://datatracker.ietf.org/doc/html/rfc4252

[4] Tatu Ylonen; C. Lonvick, «The Secure Shell (SSH) Transport Layer Protocol». [Онлайн]. Доступно на: https://datatracker.ietf.org/doc/html/rfc4253

[5] Tatu Ylonen, «How SSH port became 22». [Онлайн]. Доступно на: https://www.ssh.com/academy/ssh/port

[6] Rivest R.; Shamir A.; Adleman L, «A method for obtaining digital signatures and public-key cryptosystems». doi: doi:10.1145/359340.359342.