Расширение TLS 1.3 `compress_certificate` (RFC 8879)

Нихлебов Иван

В протоколе TLS версии 1.3 реализовано обеспечение безопасности сетевых соединений, ориентированное на снижение латентности и устранение известных криптографических уязвимостей предыдущих версий. Одним из элементов TLS-рукопожатия является передача сертификатов X.509, используемых для аутентификации сторон соединения. Несмотря на архитектурные улучшения TLS 1.3, объём передаваемых сертификатов по-прежнему остаётся значительным, что негативно сказывается на эффективности установления защищённых соединений.

Проблема

В процессе TLS-рукопожатия сервер передаёт клиенту сообщение `Certificate`, содержащее цепочку сертификатов, включающую серверный сертификат и, как правило, один или несколько промежуточных сертификатов удостоверяющих центров. Размер таких данных может составлять несколько десятков килобайт. В условиях сетей с высокой задержкой или ограниченной пропускной способностью это приводит к увеличению времени установления соединения.

В TLS 1.3 отсутствует механизм сжатия данных на уровне record layer, поскольку подобные механизмы в предыдущих версиях протокола приводили к уязвимостям классов CRIME и BREACH. В результате сертификаты передаются в несжатом виде, что создаёт проблему избыточного трафика при сохранении высоких требований к безопасности.

Концепт решения

Для устранения указанного недостатка в RFC 8879 было предложено расширение TLS 1.3 `compress_certificate`. Оно основано на идее применения сжатия исключительно к сертификатам и только на уровне сообщений рукопожатия. Клиент сообщает серверу перечень поддерживаемых алгоритмов

сжатия, после чего сервер может выбрать один из них и передать сертификаты в сжатом виде.

Данный подход позволяет существенно сократить объём передаваемых данных без повторного внедрения общего сжатия TLS-трафика. Поскольку сжимаются только публичные данные сертификатов, расширение не создаёт предпосылок для утечек секретной информации и не снижает криптографическую стойкость протокола.

Детали решения

Поддержка расширения `compress_certificate` объявляется клиентом в сообщении `ClientHello`. В расширении указывается список алгоритмов сжатия, которые клиент способен обработать. RFC 8879 определяет использование алгоритмов `zlib`, `brotli` и `zstd`.

Если сервер выбирает применение сжатия, он заменяет стандартное сообщение `Certificate` сообщением `CompressedCertificate`. Это сообщение содержит идентификатор выбранного алгоритма, длину исходных данных и сжатое представление сообщения `Certificate`. Сжатию подвергается всё тело сообщения целиком.

После получения сообщения `CompressedCertificate` клиент выполняет распаковку данных и обрабатывает результат как обычное сообщение `Certificate`. Все дальнейшие этапы TLS-рукопожатия, включая проверку цепочки доверия и криптографических подписей, выполняются без изменений.

С точки зрения безопасности расширение не ослабляет TLS 1.3. Потенциальные риски ограничиваются возможными атаками отказа в обслуживании, связанными с обработкой больших сжатых сообщений, что компенсируется стандартными ограничениями на размер входных данных.

Заключение

Расширение `compress_certificate` является эффективным механизмом оптимизации TLS 1.3, позволяющим сократить объём данных, передаваемых при установлении защищённого соединения, без ущерба для безопасности. Оно органично дополняет архитектуру современного TLS.