Расширение «Delegated Credentials» [RFC9345]

Курда Кирилл

Проблема

В современной инфраструктуре TLS серверные операторы часто развертывают TLS-терминалы в удаленных местах, таких как центры обработки данных или сети доставки контента (CDN). Это создает критическую проблему управления личными ключами: если ключ скомпрометирован в таком удаленном расположении, это может привести к взлому всех соединений, для которых этот ключ предназначен.

Традиционным решением является использование краткосрочных сертификатов, которое имеет существенные недостатки. Во-первых, краткосрочные сертификаты требуют частого обновления, что создает зависимость от удостоверяющего центра (УЦ). Если УЦ временно недоступен, сервер не сможет получить новый сертификат и, таким образом, потеряет возможность принимать новые TLS-соединения. Во-вторых, это ограничивает выбор криптографических алгоритмов подписи только теми, которые поддерживает УЦ — оператор сервера не может независимо использовать современные алгоритмы, такие как Ed25519 [RFC8032], если его УЦ их не поддерживает.

Концепт решения

Расширение Delegated Credentials решает проблему путем перехода от pull-модели (запрос авторизации при каждом подключении) к push-модели (заранее созданные DC).

Основная идея: владелец долгосрочного сертификата заранее создает краткосрочные DC и распространяет их на удаленные серверы. Они позволяют удаленному серверу самостоятельно завершать TLS Handshake без обращения к центральному серверу. Как это работает на деле:

- Владелец сертификата генерирует новую пару ключей для делегирования;
- Формируется структура DC, содержащая открытый ключ, алгоритм подписи и срок действия (не более 7 дней);
- Эта структура подписывается личным ключом долгосрочного сертификата;
- DC и соответствующий личный ключ передаются на удалённый TLS-сервер;
- При подключении клиента сервер использует личный ключ DC для завершения TLS Handshake.

- Клиент проверяет подпись DC с использованием открытого ключа из основного сертификата, а также проверяет срок их действия.

Детали решения

При установке TLS-соединения с использованием механизма DC клиент уже на этапе ClientHello объявляет поддержку данного расширения, включая расширение delegated_credential и указывая допустимые алгоритмы подписи.

В ответ сервер формирует сообщение Certificate, в котором передаёт стандартную цепочку X.509-сертификатов, завершающуюся долгосрочным сертификатом, а также структуру DC. Последняя содержит открытый ключ, срок действия, идентификатор алгоритма подписи и подпись, выполненную личным ключом основного сертификата.

Получив данные, клиент выполняет валидацию цепочки сертификатов и дополнительно проверяет DC. Проверка включает корректность подписи с использованием открытого ключа из основного сертификата, контроль того, что срок действия DC не превышает 7 дней и полностью укладывается в период валидности основного сертификата, а также соответствие используемых алгоритмов списку поддерживаемых.

После успешной проверки сервер завершает аутентификацию, формируя сообщение CertificateVerify, в котором данные Handshake подписываются личным ключом DC.

DC криптографически привязаны к конкретному сертификату. Подпись вычисляется над структурой, включающей: 64 байта заполнения (0x20), строка контекста: "TLS, server delegated credentials", байт-разделитель (0x00), DER-кодированный основной X.509 сертификат, структура DC, алгоритм подписи. Это гарантирует, что DC нельзя переиспользовать с другим сертификатом или алгоритмом.

Основной сертификат должен содержать специальное расширение DelegationUsage. Это расширение помечено как некритическое, что обеспечивает обратную совместимость — старые клиенты игнорируют его. Также сертификат должен иметь флаг digitalSignature в расширении KeyUsage.

Заключение

Расширение Delegated Credentials решает проблему управления ключами в распределенной инфраструктуре TLS путем перехода от pull-модели к push-модели. Механизм позволяет безопасно делегировать полномочия на завершение TLS-соединений без необходимости повторного обращения к удостоверяющему центру при установлении каждого TLS-соединения и без дополнительной задержки при подключении.