ЭЛВИС-ПЛЮС

Об использовании российских криптографических алгоритмов в протоколе QUIC

Протокол QUIC

ЭЛВИС-ПЛЮС

- QUIC – транспортный протокол надежной передачи данных
- QUIC v1 принят как стандарт в 2021г., описан в RFC 9000, 9001, 9002
- Обеспечивает:
  - многопотоковую передачу данных с индивидуальным управлением потоками
  - быстрое установление соединения
  - возможность динамического изменения IP-адресов и портов партнеров без разрыва соединения
  - аутентификацию партнеров, конфиденциальность и имитозащиту передаваемого трафика, шифрование заголовков пакетов

Использование QUIC для HTTP

ЭЛВИС-ПЛЮС

HTTP/3 (RFC 9114) в качестве транспорта использует только QUIC

- На март 2024 г. **29%** всех web-сайтов (и **37%** web-сайтов из “top 1000”) поддерживают HTTP/3, с тенденцией к росту ~4% в год
  https://w3techs.com/technologies/details/ce-http3
  https://w3techs.com/technologies/comparison/ce-http2,ce-http3
  Для сравнения – HTTP/2 поддерживают 35% всех web-сайтов, с тенденцией к снижению https://w3techs.com/technologies/details/ce-http2
- На январь 2024 г. **97%** всех экземпляров браузеров в мире поддерживают HTTP/3 (в том числе **95%** среди desktop и **98%** среди мобильных браузеров) https://caniuse.com/http3

Использование QUIC для других протоколов

ЭЛВИС-ПЛЮС

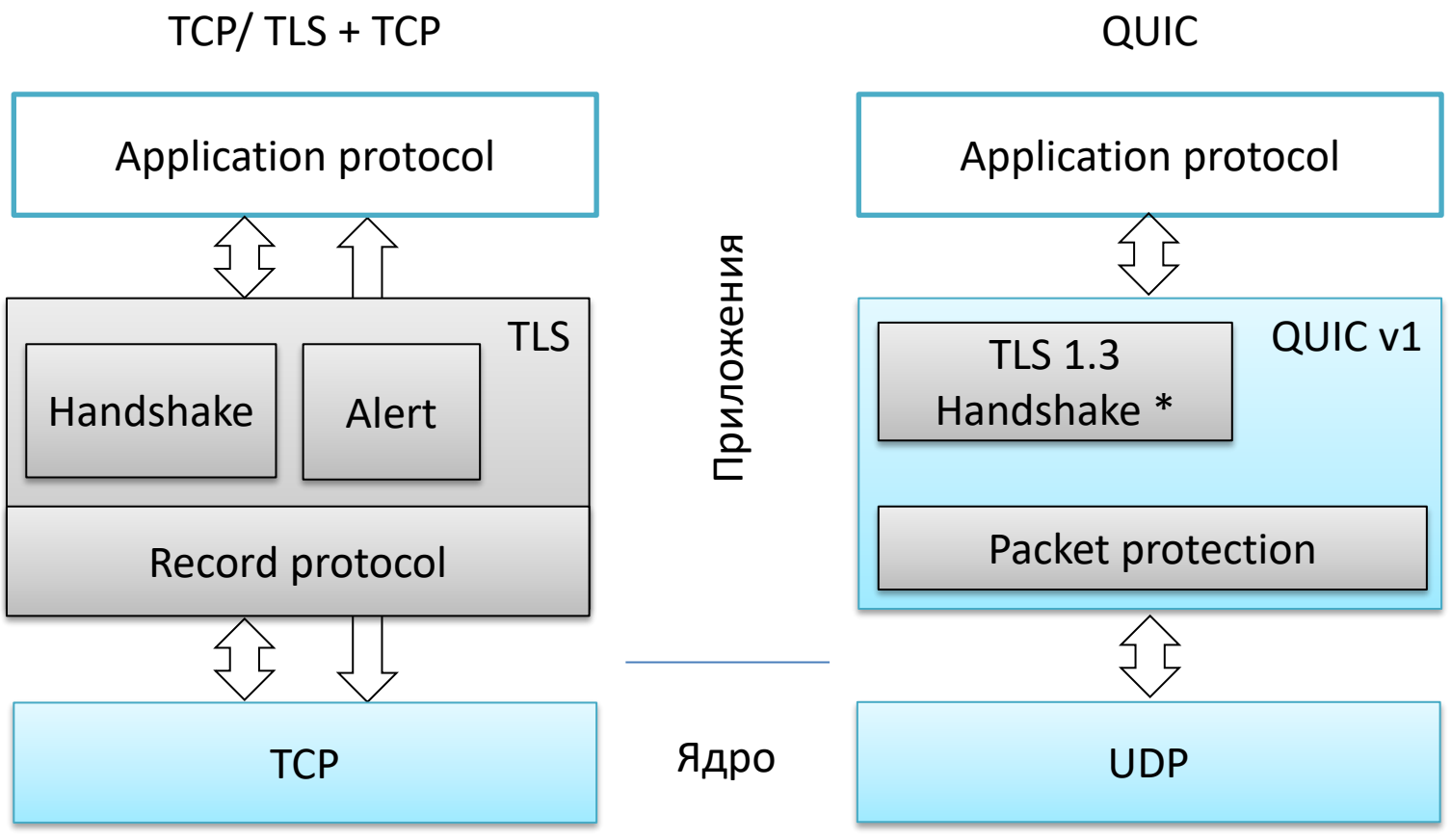
Прямое использование QUIC в качестве транспорта:

- DNS over QUIC (DoQ), RFC 9250
- BGP over QUIC, draft-retana-idr-bgp-quic
- Media over QUIC Transport, draft-ietf-moq-transport
- RTP over QUIC (RoQ), draft-ietf-avtcore-rtp-over-quic

Протоколы, оптимизированные под использование QUIC в качестве транспорта:

- Proxying UDP in HTTP, RFC 9298
- Proxying IP in HTTP, RFC 9484
- Proxying Ethernet in HTTP, draft-ietf-masque-connect-Ethernet
- Secure shell over HTTP/3 connections, draft-michel-ssh3

QUIC в иерархии сетевых протоколов



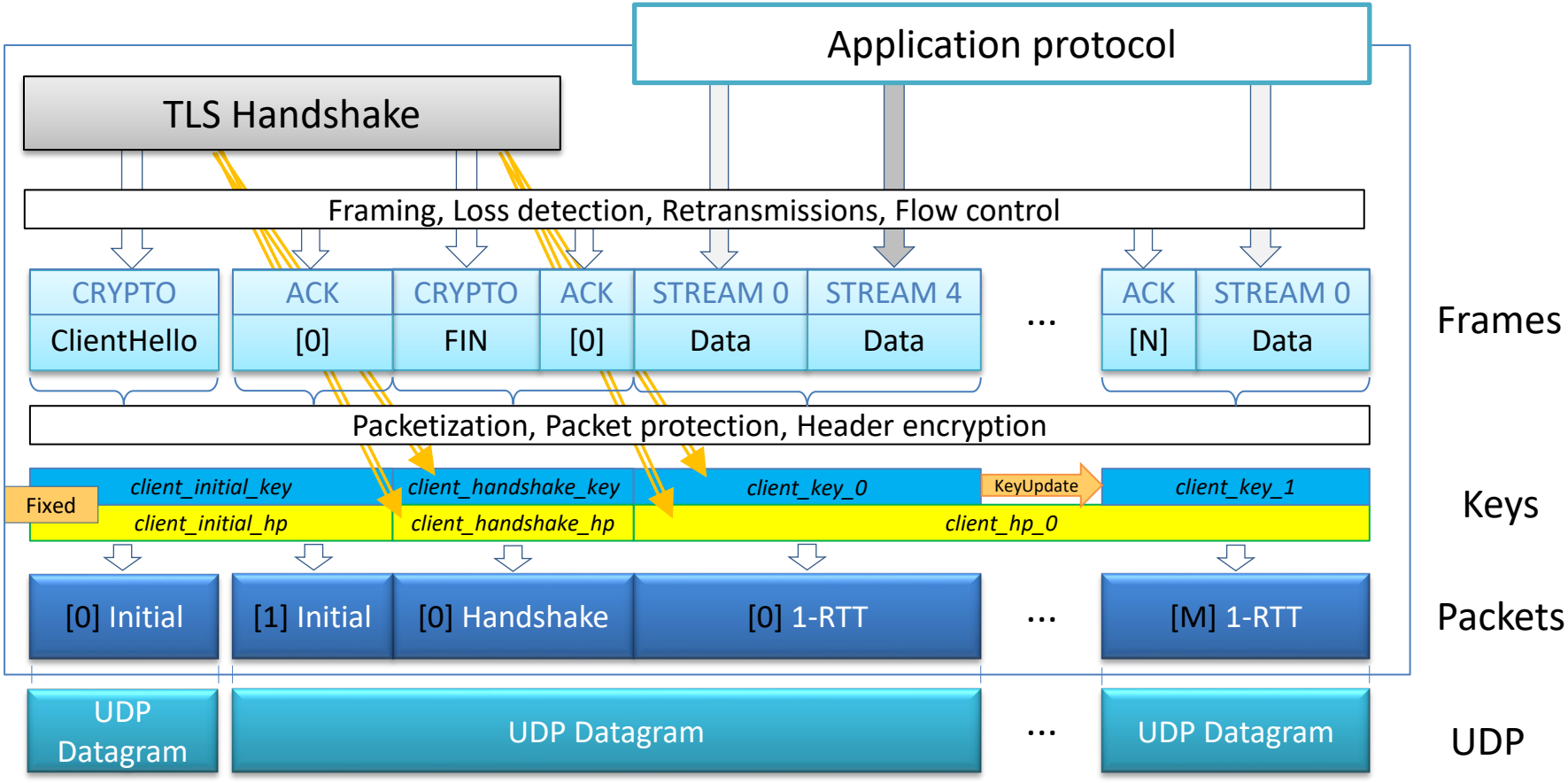
Ложка дегтя

ЭЛВИС-ПЛЮС

- QUIC сложен в реализации
- Все возможности QUIC раскрываются при использовании специфического API, соответственно требуют поддержки со стороны приложений
- QUIC использует UDP в качестве транспорта, сетевые операторы часто блокируют UDP

Структура QUIC (сообщения клиента)

ЭЛВИС-ПЛЮС



QUIC и TLS 1.3

ЭЛВИС-ПЛЮС

- QUIC использует модифицированный протокол Handshake из TLS 1.3
  - Добавлено согласование транспортных параметров QUIC в виде расширения TLS
  - HelloRetryRequest не используется (но не запрещен), вместо него используется механизм QUIC RetryPacket
  - KeyUpdate протокола TLS не используется и запрещен, вместо него используется механизм QUIC KeyUpdate, который работает на уровне защиты пакетов
  - EndOfEarlyData не используется и запрещен
  - TLS Middlebox Compatibility Mode не используется и запрещен
  - ALPN обязателен к использованию
- Протокол Alert в QUIC не используется, ошибки TLS передаются с использованием собственного механизма QUIC
- Протокол Record не используется, защита данных производится в самом QUIC
- Для протокола Handshake QUIC предоставляет защищенный транспорт с гарантированной доставкой и сохранением порядка пакетов, однако защита данных с использованием криптонаборов TLS происходит на уровне, где эти свойства отсутствуют

Ключи в QUIC

ЭЛВИС-ПЛЮС

- QUIC использует ключи, которые получает в результате выполнения TLS handshake:

  client_secret = client_handshake_traffic_secret, client_application_traffic_secret_0

  server_secret = server_handshake_traffic_secret, server_application_traffic_secret_0

  Из этих ключей QUIC вырабатывает ключи с использованием KDF:

  KDF (key, label) = HKDF-Expand-Label (key, label, “”, len)

  1. Ключ защиты пакета: *key* = KDF (*secret*, “quic key”)
  2. IV: *iv* = KDF (*secret*, “quic iv”)
  3. Ключ шифрования заголовка: *hp_key* = KDF (*secret*, “quic hp”)

Обновление ключей

ЭЛВИС-ПЛЮС

- Механизма KeyUpdate из TLS 1.3 (посредством протокола Handshake) в QUIC не используется, обновление ключей (KeyUpdate) происходит на уровне защиты пакетов
- Само обновление ключей аналогично TLS 1.3:
  *secret*_<n+1> = KDF (*secret*_<n>, "quic ku“),
  после чего пересчитываются ключ защиты пакета *key* и *iv*
- Ключ шифрования заголока *hp_key* не меняется в результате KeyUpdate
- В отличие от TLS 1.3, обновление ключей не обнуляет номеров пакетов

Защита QUIC пакетов

ЭЛВИС-ПЛЮС

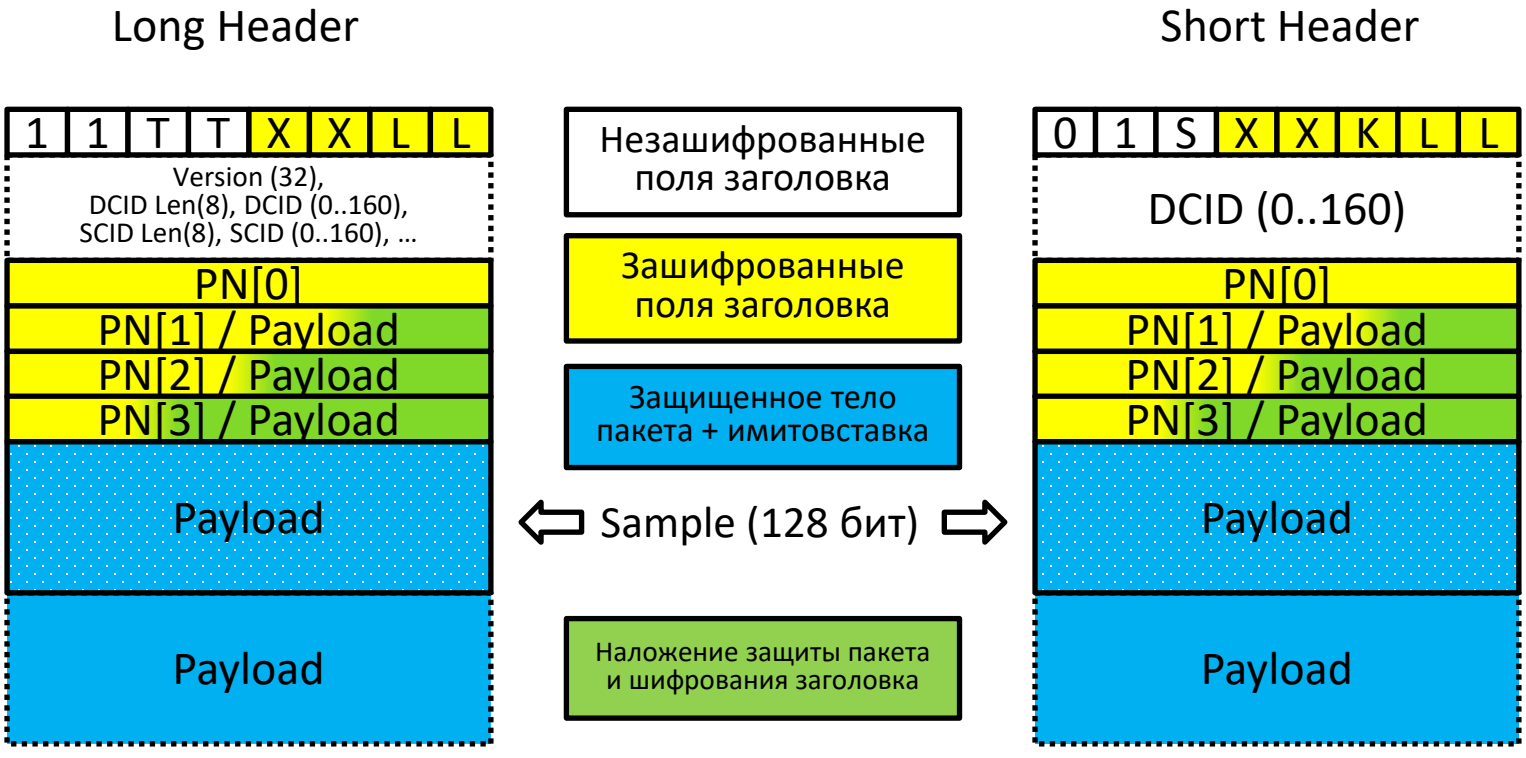
- Защита передаваемых данных в QUIC происходит на уровне пакетов
- Все пакеты (включая начальные) защищаются AEAD алгоритмом, кроме двух специальных случаев:
  - Version Negotiation Packet (не имеет защиты вообще)
  - Retry Packet (только имитозащита на фиксированном алгоритме и ключе)
- Начальные (Initial) пакеты защищаются предопределенным алгоритмом с ключом, вычисляемым из открытых данных
- Остальные пакеты защищаются алгоритмом согласованного криптонабора с ключом соответствующего уровня (handshake_traffic или application_traffic)
- Применение AEAD к пакету аналогично TLS 1.3:
  - одноразовый нонс N = <62-bit packet number> XOR IV
  - AAD = заголовок пакета
  - имитовставка добавляется после шифротекста

Шифрование заголовков пакетов

ЭЛВИС-ПЛЮС

- Применяется ко всем защищенным пакетам после их шифрования и имитозащиты
- Из зашифрованного тела пакета берется 16 байт данных, т.н. *sample*
- В качестве ключа шифрования заголовков пакетов используется отдельный ключ (*hp_key*)
- *sample* и *hp_key* используются для выработки 5-байтовой маски, которая накладывается на отдельные (в том числе битовые) поля заголовка с использованием операции XOR
- Детали выработки маски зависят от криптонабора
  - Криптонаборы с AES: *mask* = AES-ECB(*hp_key*, *sample*)[0..5]
  - Криптонаборы с Chacha20: *mask* = ChaCha20(*hp_key*, *sample*[0..3], *sample*[4..15], {0,0,0,0,0})
- Чтобы использовать криптонабор в QUIC для него должен быть определен механизм выработки маски
- QUIC предполагает, что размер имитовставки криптонабора не меньше 16 байт
  - TLS_AES_128_CCM_8_SHA256 имеет имитовставку 64 бита, в QUIC запрещен к использованию

Шифрование заголовков пакетов



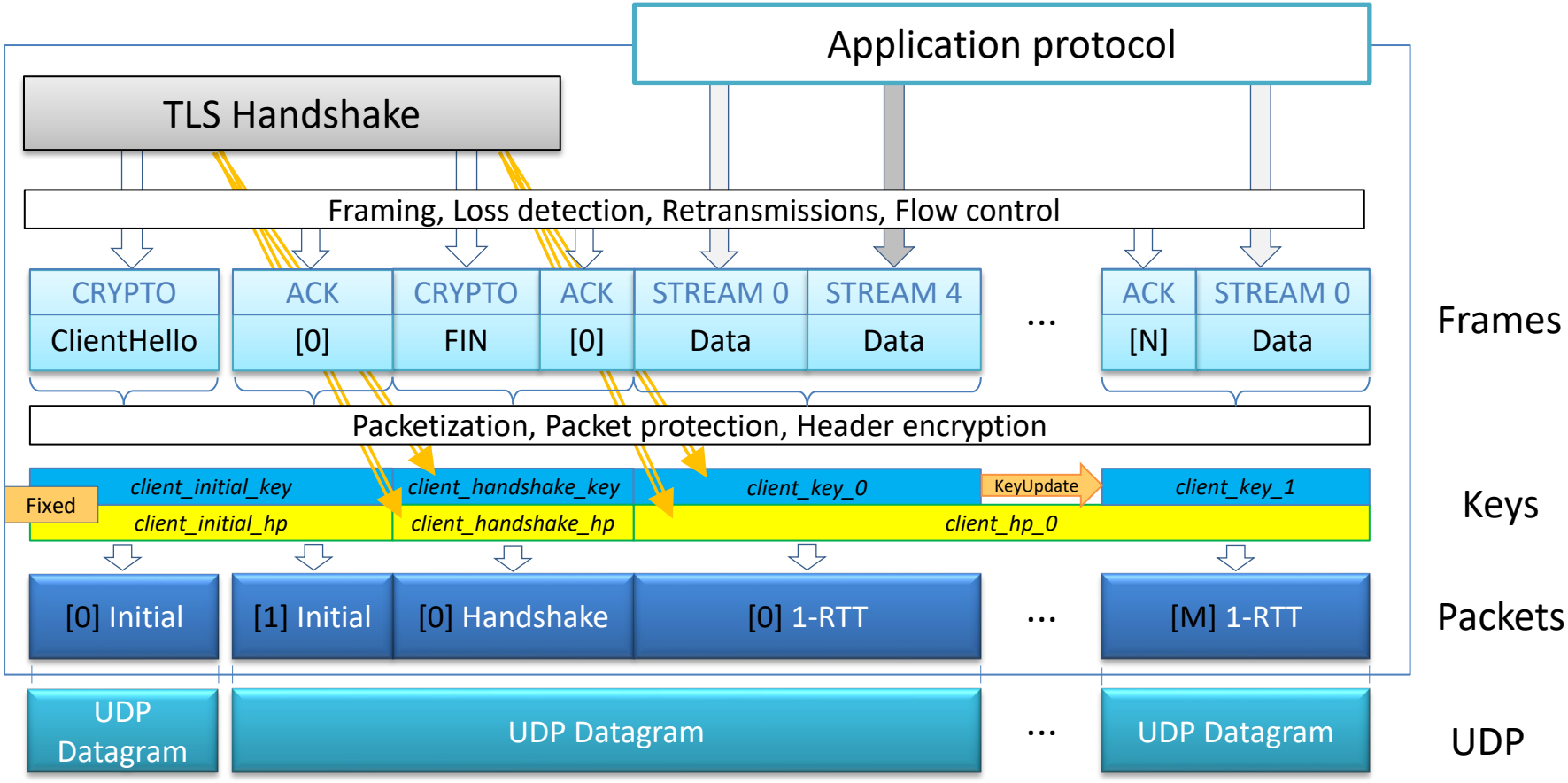
Фиксированные алгоритмы и ключи

ЭЛВИС-ПЛЮС

1. Защита начальных пакетов:
   - Используются алгоритмы **AEAD_AES_128_GCM** (AEAD), **SHA2-256** (HKDF), **AES_128_ECB** (защита заголовков пакетов)
   - *secret* = HKDF-Extract (**0x38762cf7f55934b34d179ae6a4c80cadccbb7f0a**, ***DCID***)
     client_secret = KDF(*secret*, "client in")
     server_secret = KDF (*secret*, "server in")
2. Целостность Retry пакета:
   - Используется алгоритм **AEAD_AES_128_GCM** (открытый текст нулевой длины, Retry псевдо-пакет в качестве AAD)
   - *secret* = **0xd9c9943e6101fd200021506bcc02814c73030f25c79d71ce876eca876e6fca8e**
     key = **0xbe0c690b9f66575a1d766b54e368c84e**
     iv = **0x461599d35d632bf2239825bb**

Структура QUIC (сообщения клиента)

ЭЛВИС-ПЛЮС



Криптонаборы с ГОСТ-алгоритмами

ЭЛВИС-ПЛЮС

- В Р 1323565.1.030-2020 определены 4 криптонабора с ГОСТ алгоритмами (реестр IANA для криптонаборов TLS 1.3)
- Криптонаборы основаны на шифрах Кузнечик и Магма в режиме MGM и использованием трехуровневого ключевого дерева TLSTREE с детерминированным вычислением ключа защиты трафика как функции от корневого ключа и номера защищаемой записи (для QUIC – номера пакета)
- Криптонаборы с суффиксами _L и _S отличаются нагрузкой на промежуточные ключи дерева и ключи защиты трафика

TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L
TLS_GOSTR341112_256_WITH_MAGMA_MGM_L
TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S
TLS_GOSTR341112_256_WITH_MAGMA_MGM_S

Схема защиты заголовков

ЭЛВИС-ПЛЮС

- Для криптонаборов с ГОСТ логично использовать схему выработки маски, аналогичную AES: шифрование *sample* блочным алгоритмом в режиме простой замены
- QUIC предполагает, что любой защищенный пакет содержит как минимум 16 байт псевдослучайных данных
- Поскольку защищаемые данные могут иметь минимальный размер в 1 байт, то QUIC использует только криптонаборы с имитовставкой длиной 16 байт (и более)
  - криптонаборы с Магмой оказываются в «серой зоне»

TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L
TLS_GOSTR341112_256_WITH_MAGMA_MGM_L
TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S
TLS_GOSTR341112_256_WITH_MAGMA_MGM_S

Нагрузка на ключи защиты трафика

ЭЛВИС-ПЛЮС

- Максимальный размер записи в TLS – 16 Кб; в QUIC размер пакета теоретически может достигать 64 Кбайт (ограничение UDP), но на практике обычно не превышает 1,5 Кб (типичное MTU)
- Нагрузка на ключи защиты трафика на приемной стороне может существенно отличаться от нагрузки на передающей стороне – как из-за пропадания и размножения пакетов в сети, так и в результате атаки – посылки нарушителем произвольных пакетов для анализа ключа по побочным каналам
  - Шифрование заголовков позволяет снизить риски такой атаки, но это затратно по ресурсам

TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L
TLS_GOSTR341112_256_WITH_MAGMA_MGM_L
TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S
TLS_GOSTR341112_256_WITH_MAGMA_MGM_S

Нагрузка на ключ шифрования заголовка

ЭЛВИС-ПЛЮС

- Ключ шифрования заголовков не меняется при KeyUpdate, он используется все время жизни соединения
  - Большая вероятность превышения нагрузки для долгоживущих соединений (особенно для криптонаборов _S)
  - Компрометация ключа шифрования заголовка не должна приводить к катастрофическим последствиям

TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L
TLS_GOSTR341112_256_WITH_MAGMA_MGM_L
TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S
TLS_GOSTR341112_256_WITH_MAGMA_MGM_S

Обход ключевого дерева

ЭЛВИС-ПЛЮС

- Для каждого из криптонаборов определена величина SNMAX – максимальной значение номера записи (пакета), по достижении которой должен обновляться корневой ключ (с помощью KeyUpdate)
- В отличие от TLS, после KeyUpdate номер пакета не сбрасывается в 0, что может быть неожиданным для конкретных реализаций СКЗИ

TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L
TLS_GOSTR341112_256_WITH_MAGMA_MGM_L
TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S
TLS_GOSTR341112_256_WITH_MAGMA_MGM_S

Выводы

ЭЛВИС-ПЛЮС

Для использования в QUIC криптонаборов с ГОСТ алгоритмами необходимо:

1. Определить этих криптонаборов схему шифрования заголовков
2. Провести анализ возможности использования существующих криптонаборов в ситуации, когда ошибки проверки имитовставки не приводят к закрытию сессии
3. Провести анализ влияния короткой имитовставки на шифрование заголовков (Магма)
4. Проанализировать возможность превышения нагрузки на на ключ шифрования заголовков и последствия этого
5. Учесть в СКЗИ, что номер записи (пакета) не сбрасывается при обновлении ключей
6. Обосновать возможность использования алгоритмов AES и SHA2-256 для тех ситуаций, где они применяются в QUIC

TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L
TLS_GOSTR341112_256_WITH_MAGMA_MGM_L
TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S
TLS_GOSTR341112_256_WITH_MAGMA_MGM_S

ЭЛВИС-ПЛЮС

Благодарю за внимание!

Смыслов Валерий Анатольевич

svan@elvis.ru
+7 (495) 276-0211