Протокол TLS 1.3

Компьютерные сети

Протокол TLS 1.3

TLS 1.3 – современная версия протокола TLS:

- RFC 8446, 2018 год
- В стадии внедрения

Рост использования TLS:

- 2008, TLS 1.2 – отдельные страницы сайтов
- 2018, TLS 1.3 – зашифрованы 80% трафика в Chrome*, 70% трафика в FireFox**

Проблемы TLS 1.2:

- Низкая производительность
- Атаки на TLS (RFC 7457): POODLE, BEAST, CRIME, BREACH, Renegotiation, Triple Handshake

*https://transparencyreport.google.com/https/overview
**https://letsencrypt.org/stats/

Повышение безопасности в TLS 1.3

Проблемы с безопасностью в TLS 1.2:

- TLS 1.2 можно настроить так, чтобы обеспечить высокую безопасность
- При настройке очень легко ошибиться
- TLS 1.2 поддерживает большое количество устаревших технологий для обратной совместимости

Проектные решения в TLS 1.3:

- Безопасность имеет более высокий приоритет по сравнению с обратной совместимостью
- В TLS 1.3 запретили использовать небезопасные криптографические технологии

Повышение безопасности в TLS 1.3

Набор шифров:

- В TLS 1.3 запретили использовать устаревшие алгоритмы шифрования (RC4, MD5, SHA-1 и т.п.)

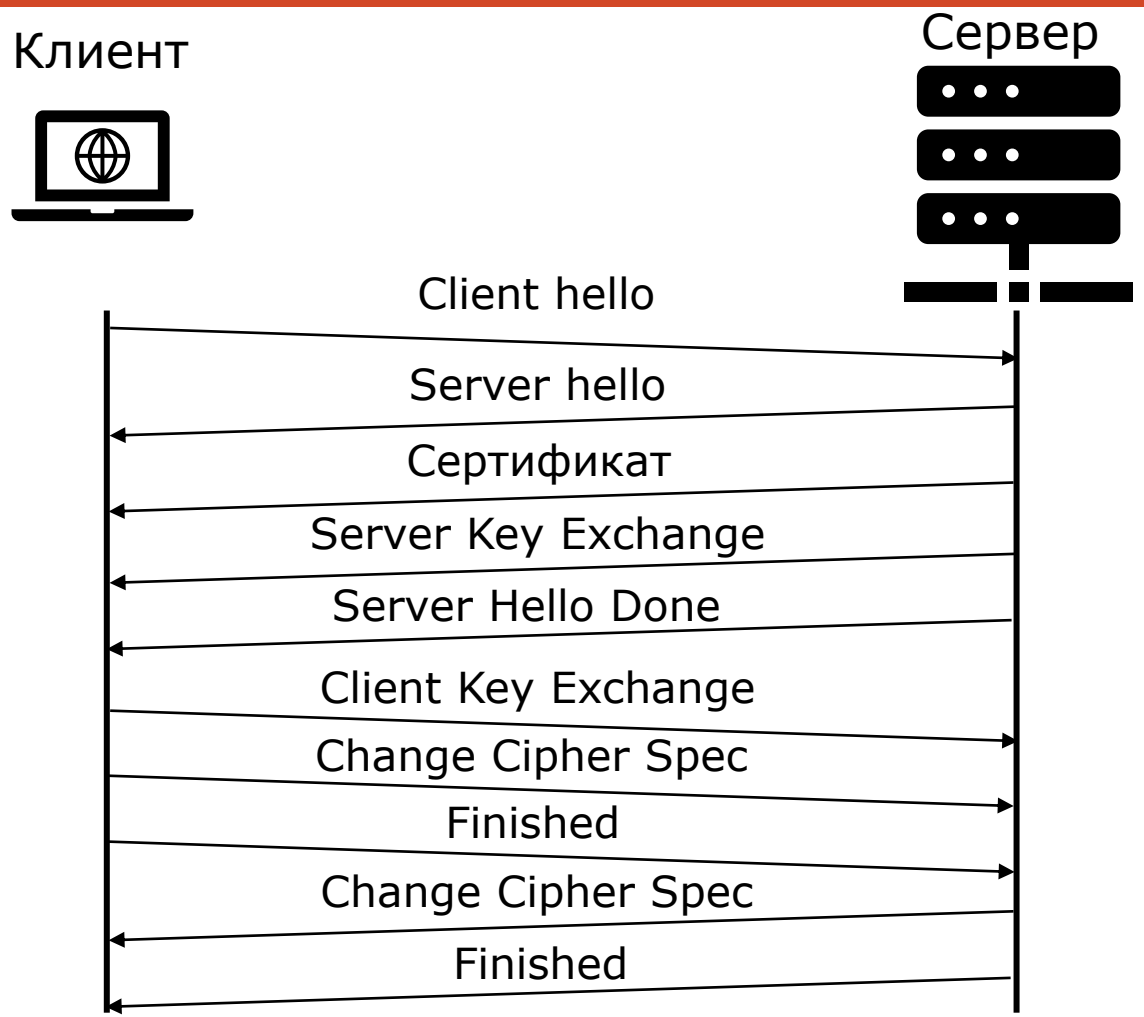
Шифры AEAD (Authenticated Encryption with Associated Data):

- Обеспечивает одновременно шифрование и MAC
- AES-GCM, Chacha20-Poly1305 (RFC 7539)

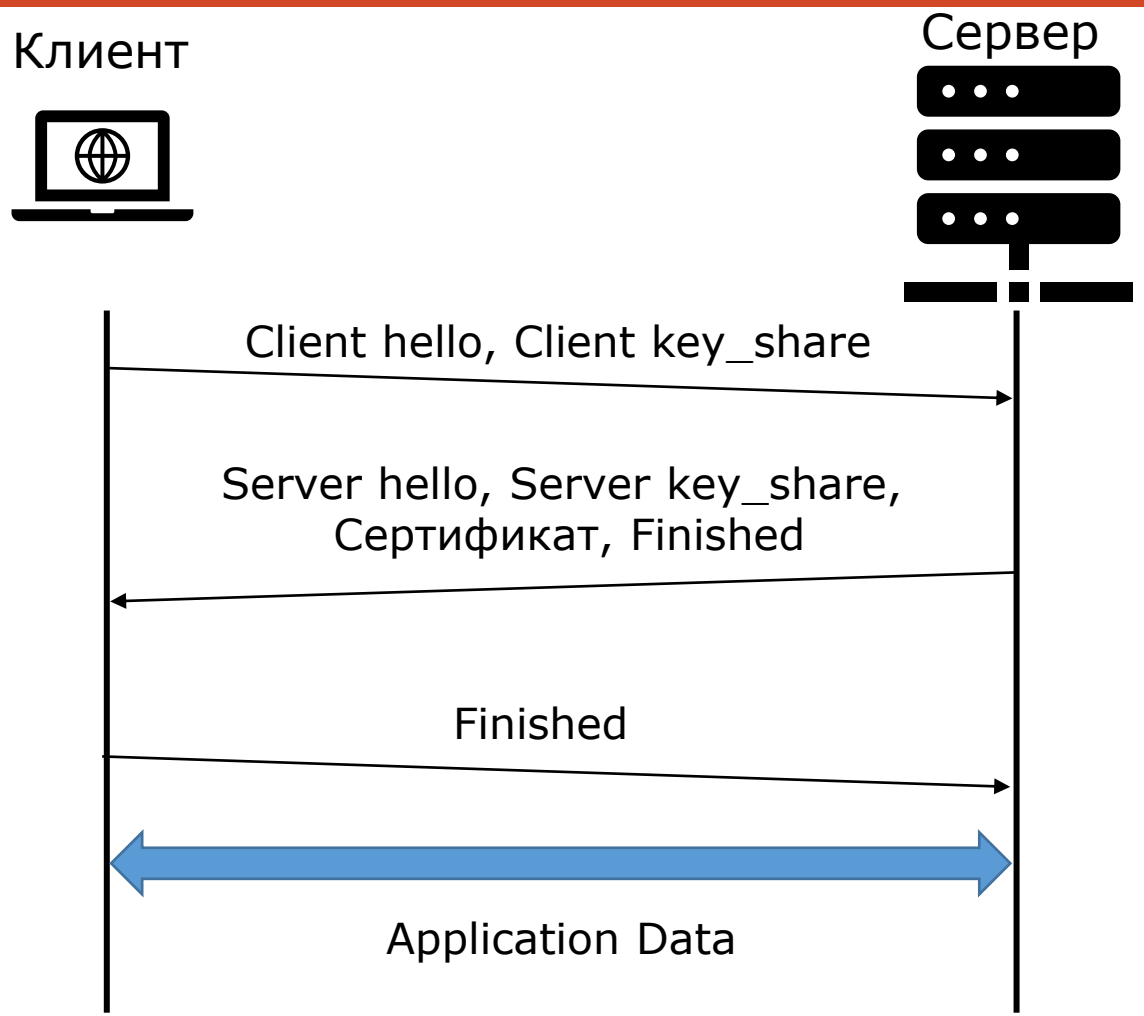
Совершенная прямая секретность:

- В TLS 1.3 обязательна
- Запрещен алгоритм обмена ключами RSA и алгоритм Диффи-Хеллмана со статическими параметрами

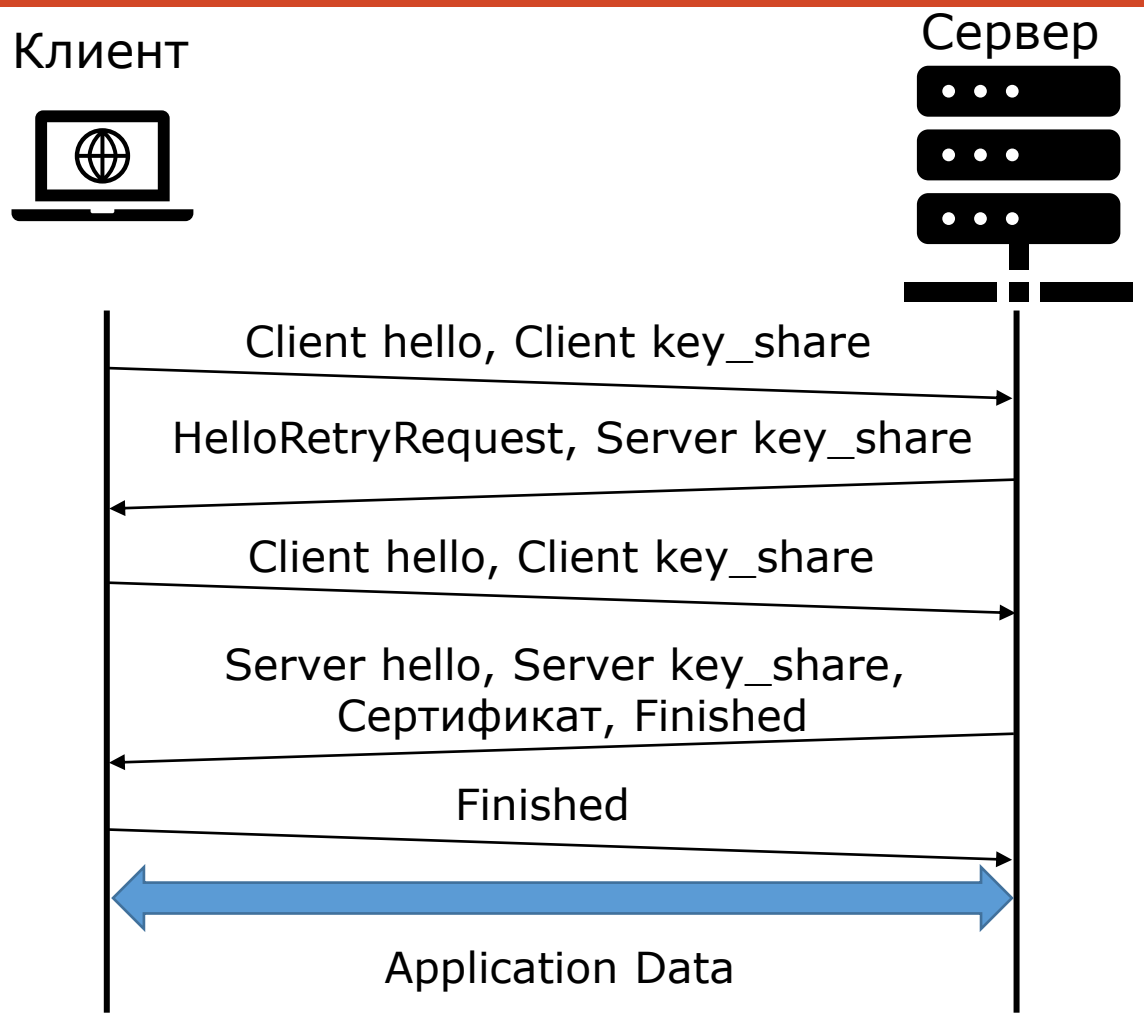
Установка соединения в TLS 1.2



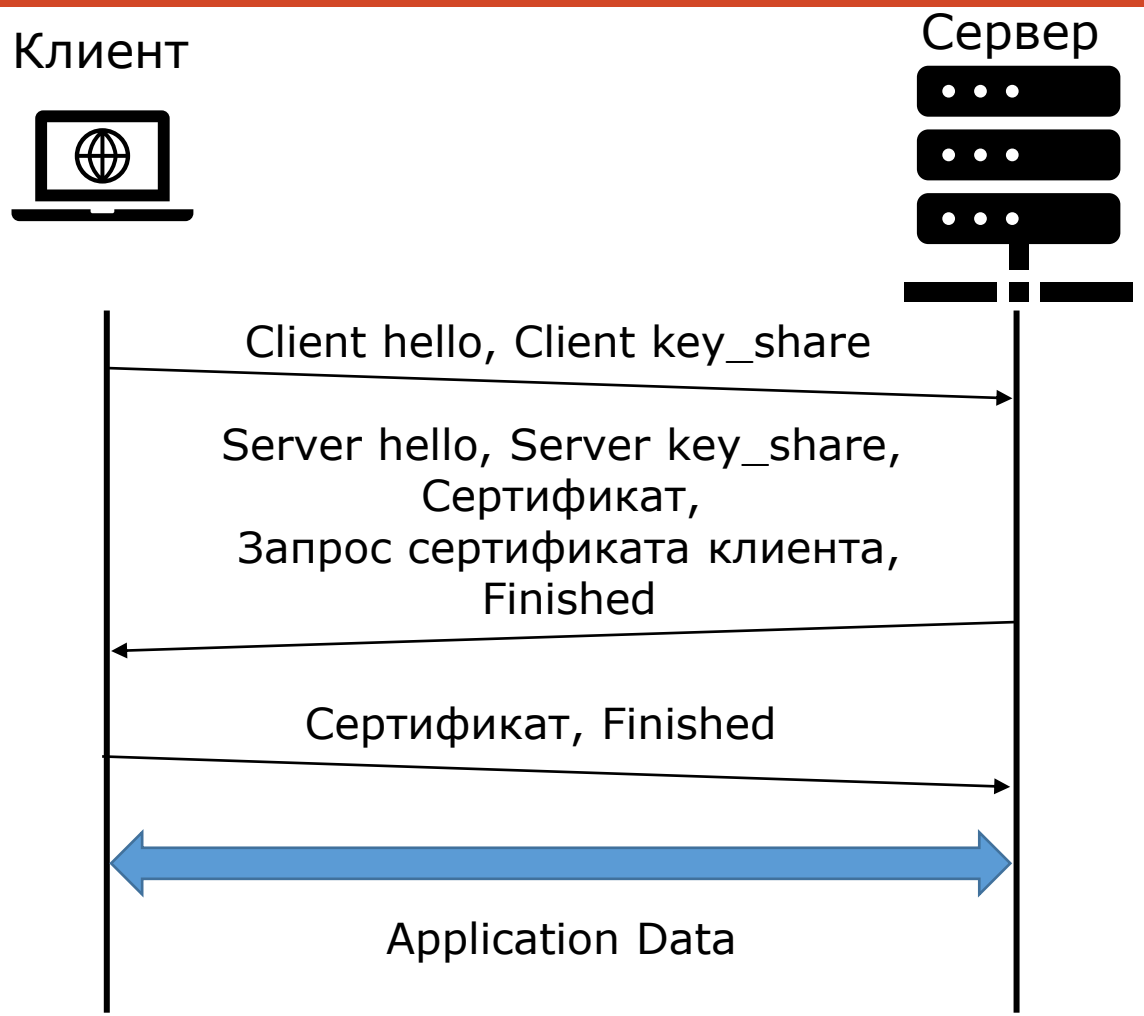
Установка соединения в TLS 1.3



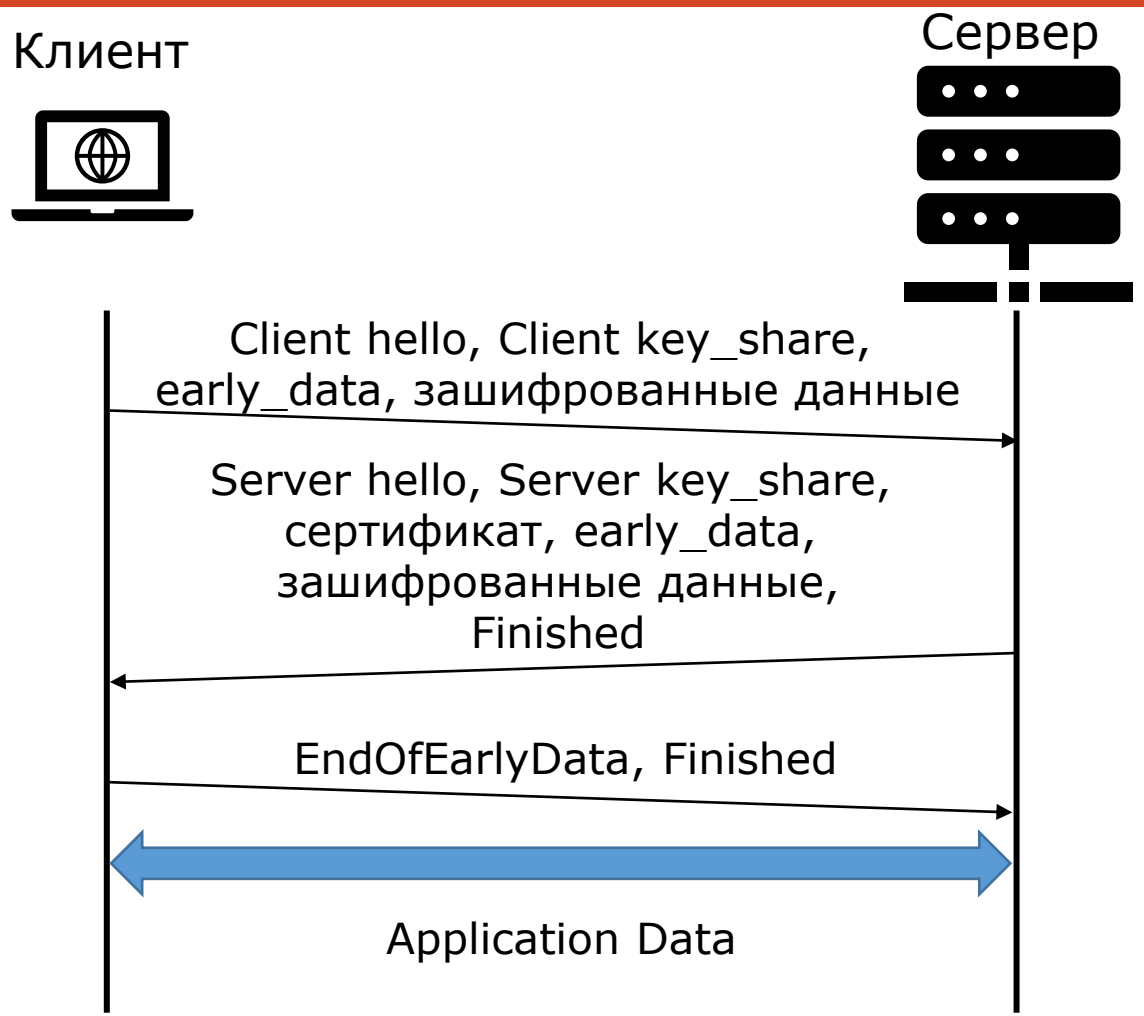
Установка соединения в TLS 1.3



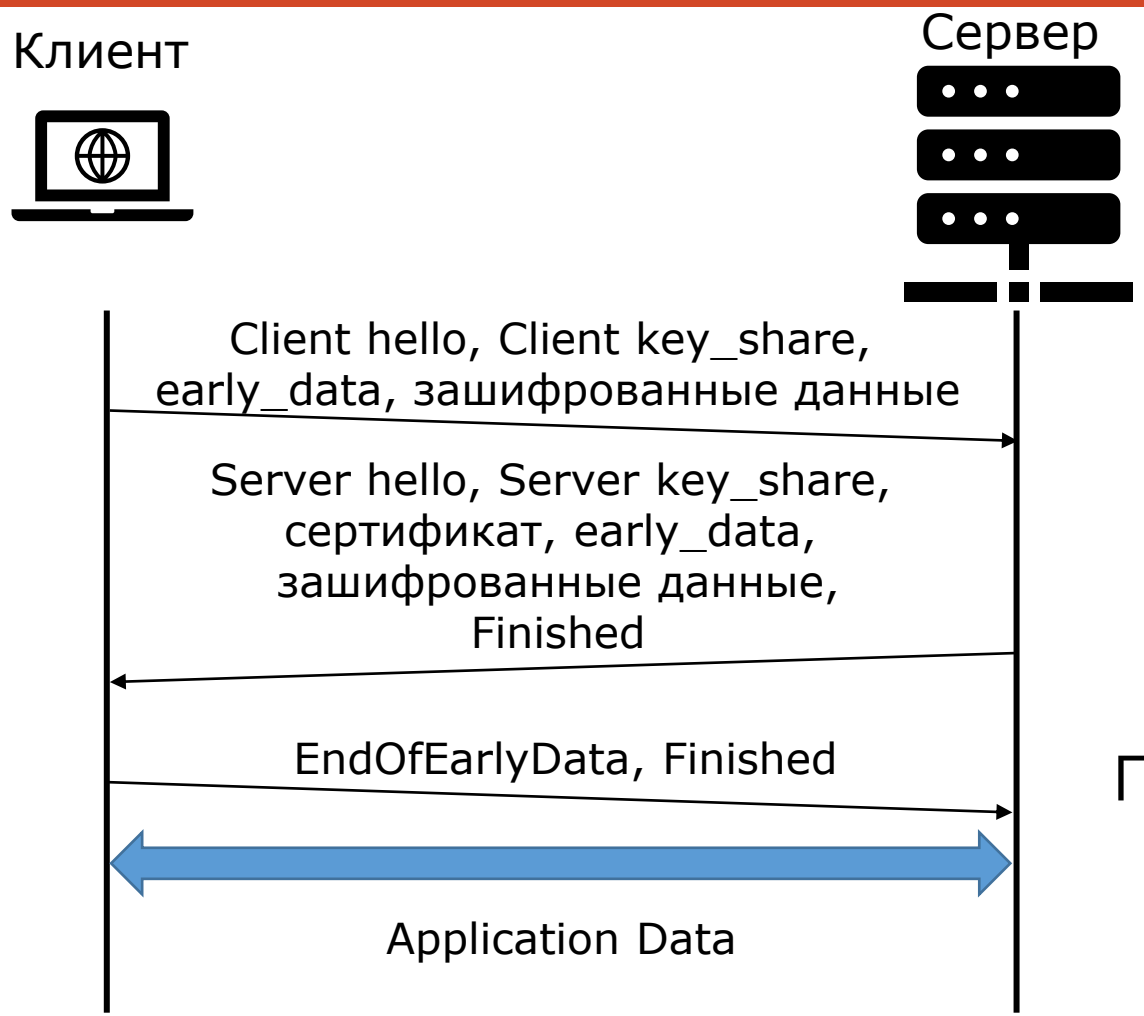
Аутентификация клиента в TLS 1.3



0-RTT в TLS 1.3


Клиент
Сервер
Client hello, Client key_share,
early_data, зашифрованные данные
Server hello, Server key_share,
сертификат, early_data,
зашифрованные данные,
Finished
EndOfEarlyData, Finished
Application Data

0-RTT в TLS 1.3



Проблемы в 0-RTT:

- Нет совершенной прямой секретности
- Возможна replay attack

Итоги

Протокол TLS 1.3:

- Современная версия TLS, в процессе внедрения
- Изменения вызваны стремительным ростом применения TLS

Увеличение безопасности:

- Совершенная прямая секретность
- Запрет устаревших шифров
- Шифры AEAD

Увеличение производительности:

- Упрощение и сокращение процесса установки соединения
- Восстановление сессии TLS с помощью 0-RTT