Протоколы TLS/SSL
Введение

Компьютерные сети

Протоколы TLS/SSL

Протоколы безопасной передачи данных в Интернет:

- TLS – Transport Layer Security, протокол защиты транспортного уровня
- SSL – Secure Sockets Layer, уровень защищенных сокетов (устарел)

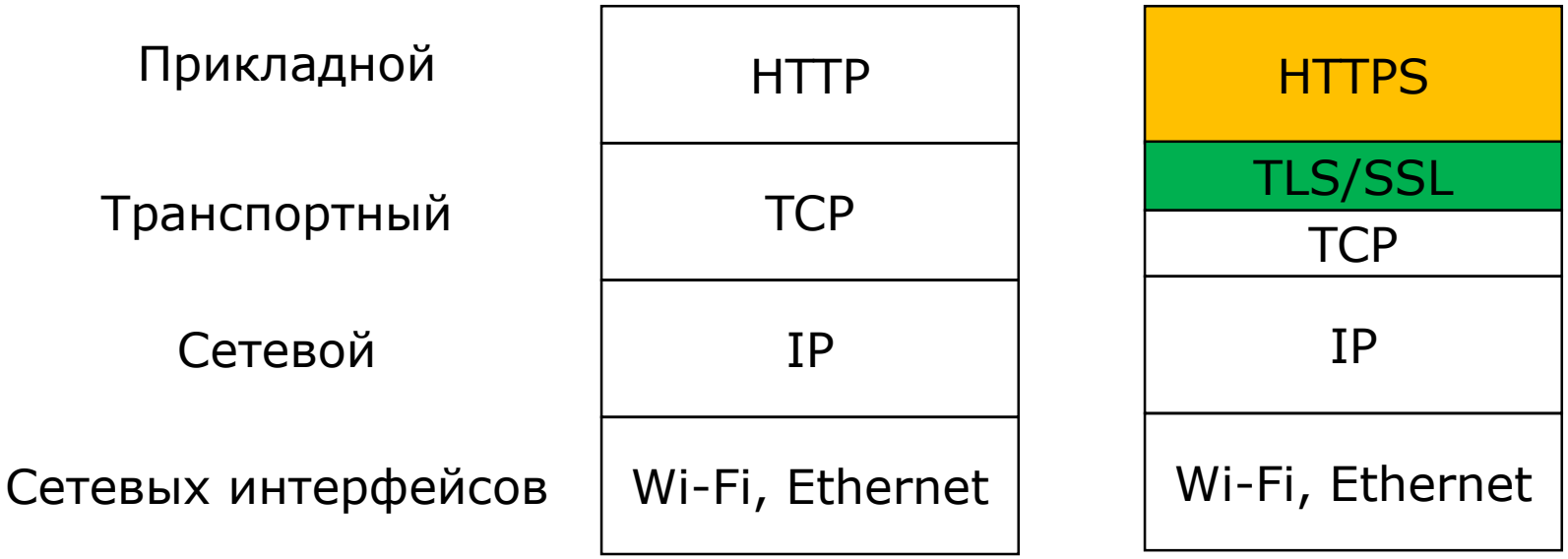
Назначение протоколов:

- Обеспечить безопасную передачу данных в небезопасной сети

Использование протоколов TLS/SSL:

- HTTPS - Hypertext Transfer Protocol Secure
- SMTPS, POP3S, IMAPS – защищенные протоколы электронной почты

Место в модели TCP/IP



Уровни модели TCP/IP

Место в модели OSI

Транспортный уровень:

- Передача данных между процессами

Сеансовый уровень:

- Восстановление сеанса шифрования, который был установлен ранее для повышения производительности

Уровень представления:

- Представление данных в зашифрованном виде при передаче по сети

История TLS/SSL

Разработка Netscape:

- SSL 1.0 – 1994 год, не был опубликован
- SSL 2.0 – 1995 год
- SSL 3.0 – 1996 год, RFC 6101

Стандартизация IETF (Internet Engineering Task Force):

- TLS 1.0 – 1999, RFC 2246
- TLS 1.1 – 2006, RFC 4346
- TLS 1.2 – 2008, RFC 5246
- TLS 1.3 – 2018, RFC 8446

Текущее состояние:

- Действующие версии протокола: TLS 1.3 и TLS 1.2
- Устаревшие версии: TLS 1.1, TLS 1.0, все версии SSL

Приватность (privacy)

Приватность (privacy)

Приватность (privacy)

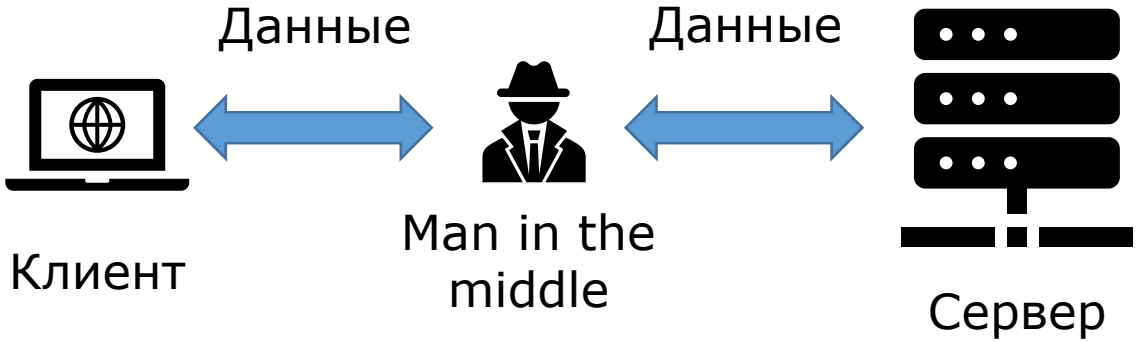
Инструмент защиты: шифрование

Целостность (integrity)

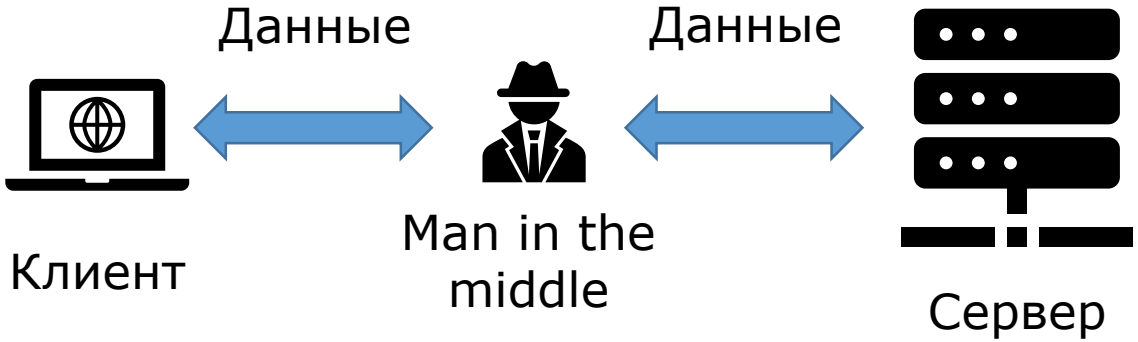
Целостность (integrity)

Инструмент защиты: хэш-функции

Аутентификация (authentication)



Аутентификация (authentication)

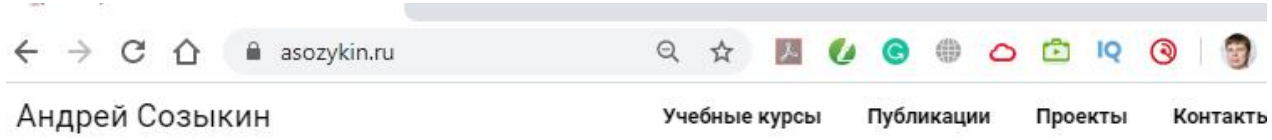


Инструменты защиты: цифровая подпись, инфраструктура открытых ключей (public key infrastructure, PKI)

Как использовать TLS/SSL

Выделенный порт:

- HTTP – порт 80
- HTTPS – порт 443



Операция STARTTLS:

- SMTP

Итоги

TLS/SSL – протоколы безопасной передачи данных по небезопасной сети:

- Приватность, целостность, аутентификация

Терминология:

- Актуальные версии протокола: TLS 1.2 и 1.3
- SSL используется как название: OpenSSL, LibreSSL

Технологии:

- Шифрование, криптографические хэш-функции, электронная подпись, сертификаты открытого ключа

Протокол TLS:

- Правила совместного использования технологий для обеспечения безопасной передачи данных