**Протоколы TLS/SSL**

TLS/SSL это семейство протоколов, которые были созданы для обеспечения безопасной передачи данных в интернете.

TLS – Transport Layer Security - протокол защиты транспортного уровня

SSL – Secure Sockets Layer - уровень защищенных сокетов (устарел, использовался до TLS)

Традиционные протоколы интернета не предпринимают ничего для безопасности, они разрабатывались очень давно, когда проблема безопасного взаимодействия не стояла. Протоколы TLS/SSL специально были разработаны для того, чтобы использоваться в небезопасных сетях. В небезопасных сетях могут действовать злоумышленники – они могут смотреть, перехватывать и менять данные, и не смотря на такое состояние сети эти протоколы должны обеспечивать безопасное взаимодействие.

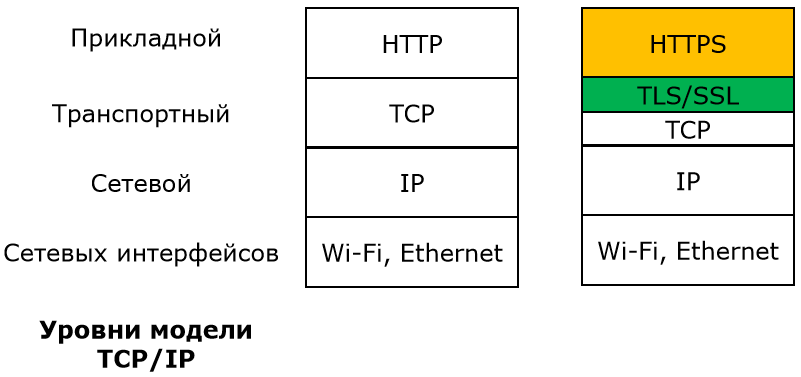
Протоколы TLS/SSL используются протоколами прикладного уровня для передачи данных:

HTTPS - Hypertext Transfer Protocol Secure (защищённая версия протокола HTTP)

SMTPS, POP3S, IMAPS – защищенные протоколы электронной почты

**Место в модели TCP/IP**

Как можно понять их названия, протокол TSL (Transport Layer Security) находится на транспортном уровне модели TCP/IP.



В свою очередь, для передачи данных по незащищенной сети, TLS/SSL используют протокол TCP, и если в традиционной схеме, прикладные протоколы, например HTTP работают напрямую с протоколом транспортного уровня TCP, то протокол TLS поверх TCP обеспечивает защищенное соединение, и именно уже с таким защищенным соединением работают протоколы прикладного уровня, например HTTP. Также на прикладном уровне, поверх TLS/SSL работает большое количество других протоколов.

**Что такое безопасность передачи данных?**

Есть 3 функции безопасности, которую обеспечивает TLS.

1. Приватность (privacy)



Допустим есть компьютерная сеть, по которой клиент подключается к серверу, например к серверу банка, для оплаты чего-нибудь. Злоумышленник может подключиться к этой сети прочитать данные.



Это пассивная атака, при которой не происходит никаких изменений, злоумышленник просто наблюдает за тем, какие данные передаются по сети. Но такая атака может принести большой ущерб, злоумышленник может украсть реквизиты карты, логины и пароли к сайтам и др. Чтобы защититься от атаки такого рода используется шифрование.

Инструмент защиты: шифрование

Если данные передаются по сети в зашифрованном виде, их нельзя просчитать.

2. Целостность (integrity)

В этом случае злоумышленник выполняет активную атаку – пытается изменить данные, которые мы передаем по сети. Например, мы зашли на сайт банка и пытаемся что-то оплатить.



Злоумышленник может изменить сумму, и счет и мы отправим деньги другому человеку – деньги украдут.



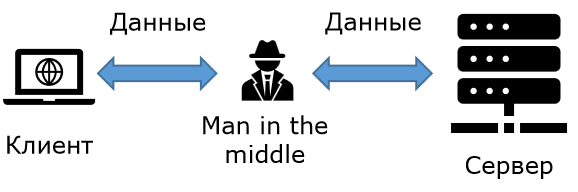
Данные, которые передаются по сети в открытом виде изменить легко, если данные зашифрованы, они также могут быть изменены. Поэтому, чтобы обеспечить целостность данных – обнаружить изменения, используются хэш-функции.

Инструмент защиты: хэш-функции.

Хэш-функция – это функция, которая по какому-то документу, или по каким-то данным другого типа генерирует строку. Как правило, документ может быть достаточно большой, а строка фиксированной длины. Свойство хэш-функции такое, что очень редко встречаются документы, для которых выдается один и тот же хэш. Таки образом, если в исходном документе что-то изменится, или будут изменения в данных, которые передаются по сети, мы возьмем от них хэш-функцию, сравним со значением хэш-функции которое нам дал отправитель, станет понятно, что данные были изменены.

2. Аутентификация (authentication)

Подтверждение того, что сервер, с которым мы общаемся, именно тот, за кого он себя выдает. Например, мы зашли на сайт банка, но как понять, что это именно он, а не какой-то другой сайт? Один из типов атаки, который часто используется на практике – man in the middle – человек по середине, или атака посредника.



В этом случае, мы отправляем данные на сервер, но наш запрос к данным перехватывает человек по середине, и после этого он отправляет от нашего имени запрос на сервер.



Таким образом, мы считаем, что мы взаимодействуем с сервером, например с банком, банк считает, что взаимодействует с вами, а на самом деле все взаимодействие происходит через посредника, который может расшифровывать все ваши данные, изменять их и передавать на сервер.

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

В протоколах TLS/SSL используют технологию цифровой подписи, которая позволяет убедиться, что мы получили данные, именно от того, от кого эти данные ждем.

Инфраструктура открытых ключей создаётся для того, чтобы мы могли узнать, что та электронная подпись, которой подписано сообщение, действительно принадлежит банку, а не злоумышленнику, который перехватил сообщение от банка, и вставил вместо цифровой подписи банка свою.

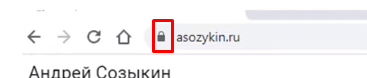
Как использовать TLS/SSL

Есть 2 варианта.

Первый вариант используется в протоколе HTTP это выделенный порт. Обычные сервер HTTP работает на порте 80. Если мы используем защищенное соединение в протоколе HTTPS, то такой сервер работает на порте 443. Если мы подключимся к 80му порту, то протокол HTTP будет использовать TCP, и передавать данные без защиты, а если подключаемся к порту 443, то здесь работает защищенный вариант протокола HTTPS, который использует TLS для передачи данных.

Второй вариант использования протокола TLS для защищенной передачи данных прикладным протоколом, это использование операции STARTTLS. В этом случае сервер работает на обычном порту, например сервер SMTP работает на 25 порту, мы сначала подключаемся к этому серверу, устанавливаем незащищенное соединение, и дальше у нас есть выбор, или передавать данные в незащищенном виде, или вызвать операцию STARTTLS, после этого протокол SMTP установит соединение TLS, и будет передавать данные по защищенному соединению а не напрямую по протоколу TCP.

Определить, что используется защищенное соединение HTTPS и TLS в браузере можно по замку:



**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