HTTPS

Трубопровод

Когда браузер делает запрос к Вашему любимому веб-сайту, этот запрос должен пройти через множество различных сетей, любая из которых может быть потенциально использована для прослушивания или для вмешательства в установленное соединение.

Запросы переданные посредством обычного HTTP (в котором и запрос клиента, и ответ сервера) передаются в открытом виде.

Но когда по каналу связи передается исключительно важная информация (такая как, пароли или данные кредитных карт), необходимо обеспечить дополнительные меры, предотвращающие прослушивание таких соединений.

Transport Layer Security (TLS)

TLS — наследник SSL — это такой протокол, наиболее часто применяемый для обеспечения безопасного HTTP соединения (так называемого HTTPS). TLS расположен на уровень ниже протокола HTTP.

TLS – гибридная криптографическая система. Это означает, что она использует несколько криптографических подходов, которые мы и рассмотрим далее:

1) Асимметричное шифрование (криптосистема с открытым ключом) для генерации общего секретного ключа и аутентификации (то есть удостоверения в том, что вы – тот за кого себя выдаете).
2) Симметричное шифрование, использующее секретный ключ для дальнейшего шифрования запросов и ответов.

Криптосистема с открытым ключом

Криптосистема с открытым ключом – это разновидность криптографической системы, когда у каждой стороны есть и открытый, и закрытый ключ, математически связанные между собой. Открытый ключ используется для шифрования текста сообщения в “тарабарщину”, в то время как закрытый ключ используется для дешифрования и получения исходного текста.

С тех пор как сообщение было зашифровано с помощью открытого ключа, оно может быть расшифровано только соответствующим ему закрытым ключом. Ни один из ключей не может выполнять обе функции. Открытый ключ публикуется в открытом доступе без риска подвергнуть систему угрозам, но закрытый ключ не должен попасть к кому-либо, не имеющему прав на дешифровку данных.

Криптосистема с открытым ключом

Симметричное шифрование

Защищённое соединение

Так как большинство протоколов связи может быть использовано как с, так и без TLS (или SSL), при установке соединения необходимо явно указать серверу, хочет ли клиент устанавливать TLS. Это может быть достигнуто например с помощью использования унифицированного номера порта, по которому соединение всегда устанавливается с использованием TLS (как, например, порт 443 для HTTPS). Как только клиент и сервер договорились об использовании TLS, им необходимо установить защищённое соединение.

Защищённое соединение

Основные шаги процедуры создания защищённого сеанса связи:
- клиент подключается к серверу, поддерживающему TLS, и запрашивает защищённое соединение;
- клиент предоставляет список поддерживаемых алгоритмов шифрования и хеш-функций;
- сервер выбирает из списка, предоставленного клиентом, наиболее надёжные алгоритмы среди тех, которые поддерживаются сервером, и сообщает о своём выборе клиенту;

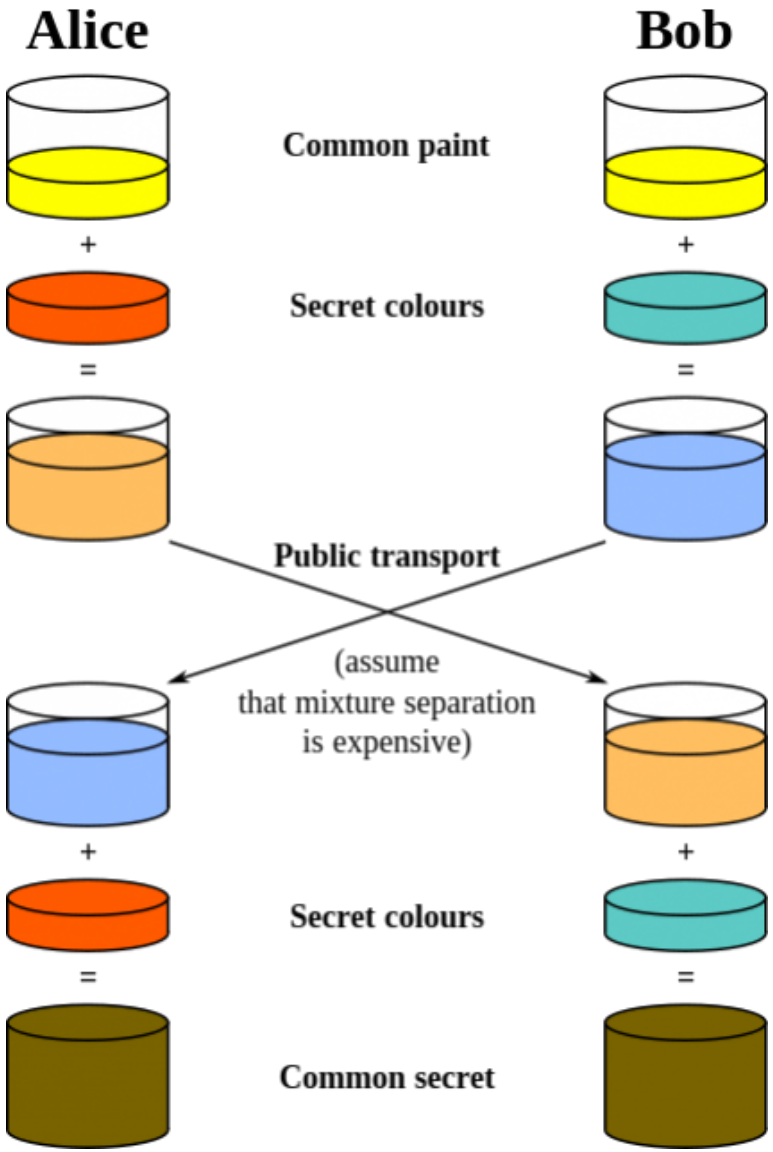
Защищённое соединение

Основные шаги процедуры создания защищённого сеанса связи:
- сервер отправляет клиенту цифровой сертификат для собственной аутентификации. Обычно цифровой сертификат содержит имя сервера, имя удостоверяющего центра сертификации и открытый ключ сервера;
клиент, до начала передачи данных, проверяет валидность (аутентичность) полученного серверного сертификата относительно имеющихся у клиента корневых сертификатов удостоверяющих центров (центров сертификации). Клиент также может проверить, не отозван ли серверный сертификат, связавшись с сервисом доверенного удостоверяющего центра;

Защищённое соединение

Основные шаги процедуры создания защищённого сеанса связи:
- для шифрования сессии используется сеансовый ключ. Получение общего секретного сеансового ключа клиентом и сервером проводится по протоколу Диффи-Хеллмана. Существует исторический метод передачи сгенерированного клиентом секрета на сервер при помощи шифрования асимметричной криптосистемой RSA (используется ключ из сертификата сервера). Данный метод не рекомендован, но иногда продолжает встречаться на практике.

Протокол Диффи — Хеллмана



Объяснение алгоритма на примере смешивания цветов.

Обратите внимание как начальный цвет (желтый) в итоге превращается в один и тот же “смешанный” цвет и у Боба, и у Алисы. Передается по открытому каналу связи базовый цвет и наполовину смешанные цвета, на самом деле бессмысленные для любого прослушивающего канал связи.

ПОЛЕЗНЫЕ ССЫЛКИ

https://ru.wikipedia.org/wiki/HTTPS - HTTPS (Wiki)
https://ru.wikipedia.org/wiki/Инфраструктура_открытых_ключей - Инфраструктура открытых ключей (Wiki)
https://ru.wikipedia.org/wiki/TLS - TLS (Wiki)
https://ru.wikipedia.org/wiki/Протокол_Диффи_—_Хеллмана - Протокол Диффи — Хеллмана
https://habr.com/post/188042/ - Как HTTPS обеспечивает безопасность соединения: что должен знать каждый Web-разработчик
http://fm4dd.com/openssl/ - Online Certificate Tools