SSL / HTTPS

немного о безопасности в сети

Что такое SSL и зачем он нужен?

SSL (Secure Sockets Layer) - Криптографический протокол, обеспечивающий безопасную передачу данных между узлами в сети.

Как работает SSL?

SSL размещен на уровне представления (6 уровень) модели OSI между протоколом прикладного уровня (например: HTTP) и протоколом транспортного уровня TCP.

SSL использует среду с несколькими слоями, что обеспечивает безопасность обмена информацией. Работу протокола можно разделить на два уровня:

1. Handshake Protocol Layer (слой протокола подтверждения подключения)
2. Record Protocol Layer (слой протокола записи)

HTTPS

Расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTPS, «упаковываются» в криптографический протокол SSL или TLS.

Handshake protocol layer

Слой состоит из нескольки подпротоколов:

1. Handshake protocol (протокол подтверждения подключения)
2. Cipher spec protocol (протокол изменение параметров шифрования)
3. Alert protocol (предупредительный протокол)

Handshake protocol (протокол подтверждения подленности)

Этот подпротокол используется для согласования данных сессии между клиентом и сервером. В данные сессии входят:

- идентификационный номер сессии;
- сертификаты обеих сторон (если такой есть у клиента);
- параметры алгоритма шифрования, который будет использован;
- алгоритм сжатия информации, который будет использоваться;
- открытый ключ;
- «общий секрет», применён для создания ключей;

Cipher spec protocol (протокол изменение параметров шифра)

Протокол изменения параметров шифрования существует для сигнализации перехода в режим шифрования. Протокол содержит единственное сообщение, которое зашифровано и сжато при текущем установленном соединении.

Alert protocol (предупредительный протокол)

Предупредительное сообщение показывает сторонам изменение статуса или о возможной ошибке. Как правило, предупреждение отсылаются тогда, когда подключение закрыто и получено неправильное сообщение, сообщение невозможно расшифровать или пользователь отменяет операцию.

Record protocol layer (слой протокола записи)

Это уровневый протокол. На каждом уровне сообщения включают поля для длины, описания и проверки. Протокол записи принимает сообщения, которые нужно передать, фрагментирует данные в управляемые блоки, разумно сжимает данные, применяя MAC (message authentication code), шифрует и передаёт результат. Полученные данные он расшифровывает, проверяет, распаковывает, собирает и доставляет к более верхним уровням клиента.

SSL сертификат

Сертификат – это цифровой способ идентификации, который выпускает центр сертификации. В сертификате содержится:

- идентификационная информация
- период действия
- публичный ключ
- серийный номер
- цифровые подписи эмитента

SSL сертификат

Проверка подленности сертификата происходит по схеме:

1. Сервер отправляет свой сертификат клиенту.
2. Клиент проверяет эмитента сертификата со списком доверительных сертифиционных центров.
3. Если эммитент в списке доверительных сертификационных центров, то клиент связываеться с этим центром и проверяет сертификат на подленность.
4. Если проверка пройдена -- клиент принимает сертификат как свидетельство подленности сервера.

symmetric-key algorithm (симмитричное шифрования)

Способ шифрования, в котором для шифрования и расшифрования применяется один и тот же криптографический ключ.

Примеры алгоритмов симметричного шифрования: AES, DES, 3DES, RC2, RC4, RC5.

Достоинства симметричного шифрования:

- высокая скорость шифрования больших обьемов данных.
- меньшая требуемая длинна ключа, для сопоставимой стойкости.
- простота реализации

symmetric-key algorithm (симмитричное шифрования)

Недостатки симметричного шифрования:

- сложность управления ключами в большой сети
- сложность обмена ключами между конечными точками

asymmetric-key algorithm (асимметричное шифрование)

Система шифрования и/или электронной подписи, при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки электронной подписи и для шифрования сообщения. Для генерации электронной подписи и для расшифровки сообщения используется закрытый ключ.

Примеры алгоритмов асимметричного шифрования: RSA, Diffie-Hellman

Hashing

Хэшфункция – это односторонняя математическая функция, которая принимает на входе сообщение произвольной длинны и вычисляет из него строку фиксированной длины.

Результатом работы хэш-алгоритма выступает значение, которое используется для проверки целостности переданных данных. Это значение создается с использованием либо MAC либо HMAC.