# Лабораторная работа №4

Принцип работы SSL

Протокол SSL использует среду с несколькими слоями, что и обеспечивает безопасность обмена информации. Конфиденциальность общения устанавливается за счёт того, что безопасное подключение открывается только целевым пользователям.

## Многослойная среда SSL

Безопасный SSL протокол размещается между двумя протоколами: протоколом, который использует программа-клиент (HTTP, FTP, IMAP, LDAP, Telnet и т.д.) и транспортным протоколом TCP/IP. Создавая своего рода заслонки с обеих сторон, он защищает и передает данные на транспортный уровень. Благодаря работе по многослойному принципу, SSL протокол может поддерживать много разных протоколов программ-клиентов.

Работу протокол SSL можно разделить на два уровня. Первый уровень – слой протокола подтверждения подключения (Handshake Protocol Layer). Он состоит из трех подпротоколов: протокол подтверждения подключения (Handshake Protocol), протокол изменения параметров шифра (Change Cipher Spec Protocol) и предупредительный протокол (Alert protocol). Второй уровень – это слой протокола записи. На рис.1 схематически изображены уровни слоев SSL


рис.1 Уровни слоёв SSL

## Уровень подтверждения подключения состоит из трех подпротоколов:

1. ***Подтверждение подключения.*** Этот подпротокол используется для согласования данных сессии между клиентом и сервером. В данные сессии входят:
* идентификационный номер сессии;
* сертификаты обеих сторон;
* параметры алгоритма шифрования, который будет использован;
* алгоритм сжатия информации, который будет использоваться;
* «общий секрет», применён для создания ключей; открытый ключ

2. ***Изменения параметров шифрования.*** Этот подпротокол используется для изменения данных ключа (keyingmaterial), который используется для шифрования данных между клиентом и сервером. Данные ключа – это информация, которая используется для создания ключей шифрования. Подпротокол изменения параметров шифрования состоит из одного единственного сообщения. В этом сообщении сервер говорит, что отправитель хочет изменить набор ключей. Дальше, ключ вычисляется из информации, которой обменялись стороны на уровне подпротокола подтверждения подключения.
3. ***Предупреждение.*** Предупредительное сообщение показывает сторонам изменение статуса или о возможной ошибке. Существует множество предупредительных сообщений, которые извещают стороны, как при нормальном функционировании, так и при возникновении ошибок. Как правило, предупреждение отсылаются тогда, когда подключение закрыто и получено неправильное сообщение, сообщение невозможно расшифровать или пользователь отменяет операцию.

Подпротокол подтверждения подключения обеспечивает реализацию многих функций безопасности. Он производит цепочку обмена данными, что в свою очередь начинает проверку подлинности сторон и согласовывает шифрование, алгоритмы хеширования и сжатия.

# Установление подлинности участников

Для определения подлинности участников обмена данных, протокол подтверждения подключения использует сертификат стандарта X.509. Это является доказательством для одной стороны, так как помогает подтвердить подлинность другой стороны, которая владеет сертификатом и секретным ключом. Сертификат – это цифровой способ идентификации, который выпускает центр сертификации. В сертификате содержится идентификационная информация, период действия, публичный ключ, серийный номер, и цифровые подписи эмитента.

**Сертификационный центр** – это третья сторона, которой по умолчанию доверяют обе стороны. При попытке установить подключение в режиме SSL сессии, сертификационный центр проверяет инициатора (обычно в этой роли выступает пользователь, компьютер клиента), а затем выдает ему сертификат. Если необходимо, сертификационный центр обновляет или конфискует сертификаты. Проверка подлинности проходит по схеме:

* клиенту предоставлен сертификат сервера;
* компьютер клиента пытается сопоставить эмитента сертификата сервера со списком доверительных сертификационных центров;
* если эмитент сертификата – доверительный сертификационный центр, то клиент связывается и этим центром и проверяет, является ли сертификат настоящим, а не подделанным;
* после проверки сертификата у сертификационного центра, клиент принимает сертификат как свидетельство подлинности сервера.

# Шифрование данных

Существует два основных способа шифрования данных: симметричный ключ (еще называется «общий секретный ключ») и ассиметричный ключ (второе название «открытый ключ» или «схема открытый-секретный ключ»). Протокол SSL использует как симметричные, так и ассиметричные ключи для шифрования данных.

**SSL-ключ** – это зашифрованные данные, которые используются для определения схемы шифрования данных во время сессии. Чем длиннее ключ, тем труднее его взломать. Как правило, алгоритмы ассиметричных ключей более стойкие их практически невозможно взломать.

**Симметричный ключ.** При шифровании симметричным ключом, используется один и тот же ключ для шифрования данных. Если две стороны хотят обмениваться зашифрованными сообщениями в безопасном режиме, то обе стороны должны иметь одинаковые симметричные ключи. Шифрование симметричным ключом обычно используется для шифрования большого объема данных, так как это процесс проходит быстрее, чем при ассиметричном шифровании. Обычно используются алгоритмы DES (Data Encryption Standard – стандарт шифрования данных), 3-DES (тройной DES), RC2, RC4, и AES (Advanced Encryption Standard – современный стандарт шифрования).

**Ассиметричный ключ.** Шифрование с применением ассиметричного (открытого) ключа использует пару ключей, которые оба были получены, пройдя целый комплекс математических вычислений. Один из ключей используется в качестве открытого, как правило, сертификационный центр публикует открытый ключ в самом сертификате владельца (обычно это является заголовком (subject)). Секретный ключ держится в тайне и никогда никому не окрывается. Эти ключи работают в паре: один ключ используется для запуска противоположных функций второго ключа. Так, если открытый ключ используется чтоб шифровать данные, то расшифровать их можно только секретным ключом. Если данные шифруются секретным ключом, то открытый ключ должен это расшифровывать. Такая взаимосвязь позволяет, используя схему шифрования открытым ключом, делать две важные вещи. Во-первых, любой пользователь может получить открытый ключ по назначению и использовать его для шифрования данных, расшифровать которые может только пользователь, у которого есть секретный ключ. Во-вторых, если заголовок шифрует данные, используя свой секретный ключ, каждый может расшифровать данные, используя соответствующий открытый ключ. Именно это является основой для цифровых подписей. Самый распространенный алгоритм, который используется при шифровании с ассиметричными ключами – RSA (назван в честь разработчиков Rivest, Shamir, Adleman).

Протокол SSL использует шифрование с открытым ключом для того, чтоб подтвердить клиенту подлинность сервера, и наоборот. Шифрование открытым ключом также используется для определения ключа сессии. Ключ сессии используется симметричными алгоритмами для шифровки большого объема данных. Это объединяет ассиметричное шифрование (для проверки подлинности) и быстрое симметричное шифрование объемных данных (что не требует больших вычислительных ресурсов и больших затрат времени).

# Хэширование

Во время подтверждения подключения согласовывается также и хэш-алгоритм. Хэш–функция – это односторонняя математическая функция, которая принимает на входе сообщение произвольной длинны и вычисляет из него строку фиксированной длины. Хеш-значение играет роль идентификационной отметки, «отпечаток сообщения». Как и отпечатки пальцев уникальны для каждого человека, хеш-значения тоже уникальны. Кроме того, как отпечатки пальцев значительно меньше, чем сам человек, так и хеш-значение намного меньше оригинального сообщения. Хэширование используется для обеспечения целостности передачи данных. Самыми популярными хэш-алгоритмами являются MD5 (Message Digest 5 – дайджест сообщения, 5 версия) и SHA-1 (Standard Hash Algorithm – стандартный алгоритм хэширования). MD5 создает 128 битное хэш-значение,

а SHA-1 создает 160 битное хэш-значение. Есть также новые, более устойчивые алгоритмы хэширования: WHIRLPOOL, SHA-512, SHA-384, HAVAL, Tiger(2).

Результатом работы хэш-алгоритма выступает значение, которое используется для проверки целостности переданных данных. Это значение создается с использованием либо MAC либо HMAC. MAC - Message Authentication Code – код проверки сообщения. Он использует отображающую функцию и предоставляет данные в виде значений фиксированного размера, а затем - хэширует само сообщение. MAC гарантирует, что данные не были изменены во время передачи. Разница между MAC и цифровой подписью состоит в том, что цифровая подпись это также способ подтверждения подлинности. SSL использует MAC.

HMAC - Hashed Message Authentication Code – хэшированный код проверки сообщения. HMAC похож на MAC, но при этом используется хэш-алгоритм вместе с общим секретным ключом. Общий секретный ключ прикрепляется к данным, которые хэшируются. Это позволяет сделать хэширование более безопасным, так как обе стороны должны иметь одинаковые секретные ключи для подтверждения подлинности данных. HMAC используется только протоколом TLC.

# Уровень записи

Протокол на уровне слоя записи получает зашифрованные данные от программы-клиента и передает его на транспортный слой. Протокол записи берет данные, разбивает на блоки размером, который подходит криптографическому алгоритму, использует MAC (или HMAC) и потом шифрует (расшифровывает) данные. При этом используется информация, которая была согласованна во время протокола подтверждения данных. В некоторых случая на этом уровне проходит сжатие (распаковка) данных.

Цифровой сертификат является своего рода паспортом в цифровом мире. В нём хранится следующая информация:

- ключи шифрования
- личные данные субъекта, такие как имя, электронный адрес, название организации
- область применения
- срок действия сертификата
- наименование Центра Сертификации ЦС (Certification authority, CA), выдавшего сертификат
- цифровую подпись ЦС, выдавшего сертификат

Этот документ используется в инфраструктуре открытых ключей в следующих случаях:

- **при создании и проверке цифровых подписей, штампов времени и т.п.** Цифровые подписи, если они верны, являются свидетельством того, что документ был подписан владельцем сертификата и после этого не был изменён по пути. Например, драйвер устройства прошёл тестирование на совместимость с операционной системой, то он подписывается Windows. Что является свидетельством того, что проблем при использовании этого драйвера в Windows не будет. Штампы времени являются достоверной отметкой времени. Цифровые подписи и штампы времени очень сложно подделать, не имея закрытого ключа. В

некоторых странах они имеют юридическую силу, в результате чего электронный документооборот превращается из мечты в реальность.
- **при шифровании.** Для этого используется открытый ключ, всегда присутствующий в сертификате получателя.
- **аутентификация.** В электронных сетях и в Интернете очень важно порой удостовериться, что никто посторонний не проник куда не надо. Например, покупателю необходимо удостоверится, что электронный магазин, в котором он хочет сделать покупку, действительно является магазином, чтобы не перечислить деньги очередному мошеннику.

Каждый сертификат имеет специфическое целевое назначение, которое ясно указано в этом документе. Применение сертификата разрешается только в этих целях.

| Область применения | Описание |
|---|---|
| Проверка подлинности сервера | Применяется серверами (например, защищёнными web-серверами, использующими протокол Secure Sockets Layer) для аутентификации самих себя по отношению к клиентам |
| Проверка подлинности клиента | Применяется клиентами (например, пользователями Web) для аутентификации самих себя по отношению к серверам |
| Подписывание кода | Используется производителями программных средств для аутентификации пользователями программ (например, элементов управления ActiveX) |
| Защищённая электронная почта | Применяется для подписывания и кодирования электронных сообщений с помощью протокола Secure/Multipurpose Internet Mail Extensions (S/MIME) |
| Подписывание документа | Применяется, например, для подписывания документов MS Office |
| Файловая система EFS | Применяется с симметричным ключом для кодирования/декодирования файлов и папок |
| Восстановление файлов | Применяется с симметричным ключом для восстановления закодированных файлов и папок |

При получении сертификатов генерируется открытый и закрытый ключи. Оба они хранятся в сертификате. Когда требуется передать кому-нибудь сертификат, то сертификат экспортируется без закрытых ключей и передаётся, чтобы никто посторонний не смог воспользоваться секретным ключом.

Для безопасного хранения сертификатов Windows использует хранилище сертификатов отдельно для каждого пользователя. Так что никто другой, включая администратора, не может воспользоваться вашими секретными ключами.

Однажды создав, или получив электронный сертификат и поместив его в хранилище человек получает возможность подписывать свои сообщения и шифровать их, не вникая в тонкости процесса.

В хранилище сертификаты хранятся в соответствии с их назначением и проявляемым к ним уровню доверия.

Логические хранилища:

| Название | Описание |
|---|---|
| Личное | Любые ваши сертификаты, используемые вами и связанные с вашими закрытыми ключами. |
| Доверенные корневые центры сертификации | Автоматически подписанные сертификаты от ЦС, которые неявным образом являются доверенными. Здесь хранятся сертификаты, изданные сторонними ЦС, Microsoft, а также вашей организацией (если организация располагает собственным сервером сертификатов) |
| Доверительные отношения в предприятии | Помещая сюда сертификаты, изданные другими организациями, вы делаете доверенными корневые сертификаты этих организаций. Что влечёт за собой автоматическое доверие любым сертификатам, изданными ими. |
| Промежуточные центры сертификации | Сертификаты, изданные другими ЦС |
| Сертификаты, к которым нет доверия | Сертификаты, которым вы явно не доверяете. Здесь обязательно находятся два сертификата выданных VeriSign, которая в марте 2001 года объявила о выдаче этих сертификатов лицу, сумевшему "войти в доверие". Также здесь хранятся сертификаты, когда вы выбираете опцию не доверять сертификату. |
| Сторонние корневые центры сертификации | Та часть основных доверенных ЦС, которые отличны от Microsoft и вашей организации. |
| Доверенные лица | Сертификаты, изданные доверенными людьми |
| Другие пользователи | Сертификаты людей, которым вы посылаете шифрованные сообщения или документы |
| Запросы заявок на сертификаты | Отложенные запросы на регистрацию сертификата |

Из хранилища Windows сертификаты можно экспортировать в любой из следующих форматов:

- **DER encoded binary X.509.** Аббревиатура от слов Distinguished Encoding Rules (Превосходные правила кодирования), DER X509 платформенно-независимый метод хранения сертификатов. Может использоваться для их передачи между компьютерами. Имеет расширение .cer и .crt.
- **Base-64 encoded X.509.** Вариант кодирования, разработанный для использования совместно с S/MIME (безопасным протоколом электронной почты). Файл использует ASCII-символы, благодаря чему может пройти неповрежденным через все почтовые шлюзы. Имеет расширение .cer и .crt.
- **Cryptographic Message Syntax Standard — сертификаты PKCS #7.** В отличие от формата X509 сертификаты стандарта PKCS #7 (Public Key Cryptography Standard — криптографический стандарт открытого ключа) позволяет сохранить не только сам сертификат, но и все сертификаты в пути сертификации. Это позволяет сохранить доверие к сертификату на другом компьютере. Имеет расширение .p7b и .spc.

- **Файл обмена личной информации (Personal Information Exchange) — PKCS #12.** Единственный формат, который может включать закрытые ключи. Непременным условием разрешения на включение закрытого ключа является то, что ключ помещается как разрешённый к экспорту. Этот формат надо использовать очень осторожно. Ни в коем случае ваш секретный ключ не должен попасть в руки к кому-нибудь. Файлы в этом формате предназначены только для вас лично. Имеет расширение .pfx и .p12.
- **Microsoft Serialized Certificate Store.** Этот формат используется только в том случае, если вы экспортируете сразу несколько сертификатов (для этого необходимо выделить желаемые сертификаты перед экспортом). Имеет расширение .sst.

Сертификаты следует экспортировать в следующих случаях:

- Для создания резервных копий своих собственных сертификатов.
- Для переноса сертификатов на другой компьютер.

Практическая часть:

Задание:

1.Посмотрите параметры сертификата "электронной сберкассы" Сбербанка - https://esk.sbrf.ru

2.Опишите, кем, на какой срок и для какого субъекта сертификат был выдан.

3.Выполните запрос личного сертификата, используя центр сертификации Thawte свободно распространяемый (trial SSL)

4.Выполните настройку, запросите сертификат X.509 и получите личный сертификат пользователя

5.Убедитесь, что сертификат был опубликован в хранилищеСертификатов

6.Создайте две учетные записи пользователей, например, User1 и User 2.

7. Зарегистрируйтесь как Администратор всистеме. Работая под первой учетной записью, запросите сертификат (если он не был получен ранее), после чего зашифруйте папку с текстовым файлом, который не жалко потерять. Проверьте, что будет происходить при добавлении файлов, переименовании папки, копировании ее на другой диск с файловой системой NTFS на том же компьютере, копировании папки на сетевой диск или диск с FAT.

8.Убедитесь, что другой пользователь не сможет прочитать зашифрованный файл.

9. Снова зайдите под первой учетной записью. В оснастке Certificates, удалите сертификат пользователя (несмотря на выдаваемые системой предупреждения). Завершите сессию пользователя в системе и войдите заново. Попробуйте открыть зашифрованный файл.

Контрольные вопросы:

1.Что такое Сертификат, и для каких целей его используют?

2.Что такое Центр сертификации?

3.Какую информацию содержат сертификаты?

4.Какие виды ЦС используются службами Windows?

5.Какие типы сертификатов используются в Интернете?

6.Что такое Хранилище сертификатов и как его можно просмотреть?

7.Какую информацию содержат папки хранилища сертификатов?

8.Зачем запрашивают сертификаты и как это сделать?

9.Как осуществляется импорт и экспорт сертификатов?