Эссе на тему: Secure Sockets Layer 3.0: Overiew and Analysis

Студента 916 группы Гаврилина Кирилла Юрьевича

Secure Sockets Layer

Internet Information Server позволяет пользователям подключаться по защищенному коммуникационному каналу благодаря поддержке протокола Secure Sockets Layer (SSL) и шифрования по алгоритму компании RSA Data Security как на сервере, так и на клиенте. На этом занятии описан уровень протокола SSL.

Пользователи, посещающие коммерческие Web-узлы, как правило, весьма неохотно предоставляют конфиденциальные сведения о себе (например, номера кредитных карт и банковских счетов), опасаясь, что кто-нибудь может перехватить эту информацию. Чтобы развеять их тревоги. Вам нужно защитить конфиденциальную информацию, которая передается по сети, от любых форм перехвата и постороннего вмешательства.

Стандарт SSL был разработан фирмой Netscape Communications. В его основе лежит шифрование с открытым ключом. Желающий воспользоваться услугами безопасности протокола SSL должен, набирая адрес порта, вместо обычного http://… набрать https://…, подсоединившись таким образом к SSL-серверу. Признаком этого будет появление значка  в нижнем углу броузера.

Протокол SSL 3.0 — одно из средств защиты Web-сервера — обеспечивает надежный защищенный канал связи с пользователем

узла. SSL гарантирует аутентификацию Вашего Web-узла клиентам и, с другой стороны, надежно идентифицирует их.

Помимо SSL, Ваш Web-сервер поддерживает протокол PCT 1.0. Подобно SSL, PCT 1.0 предоставляет в Ваше распоряжение устойчивые и надежные средства шифрования для обеспечения защиты соединения.

Архитектура SSL

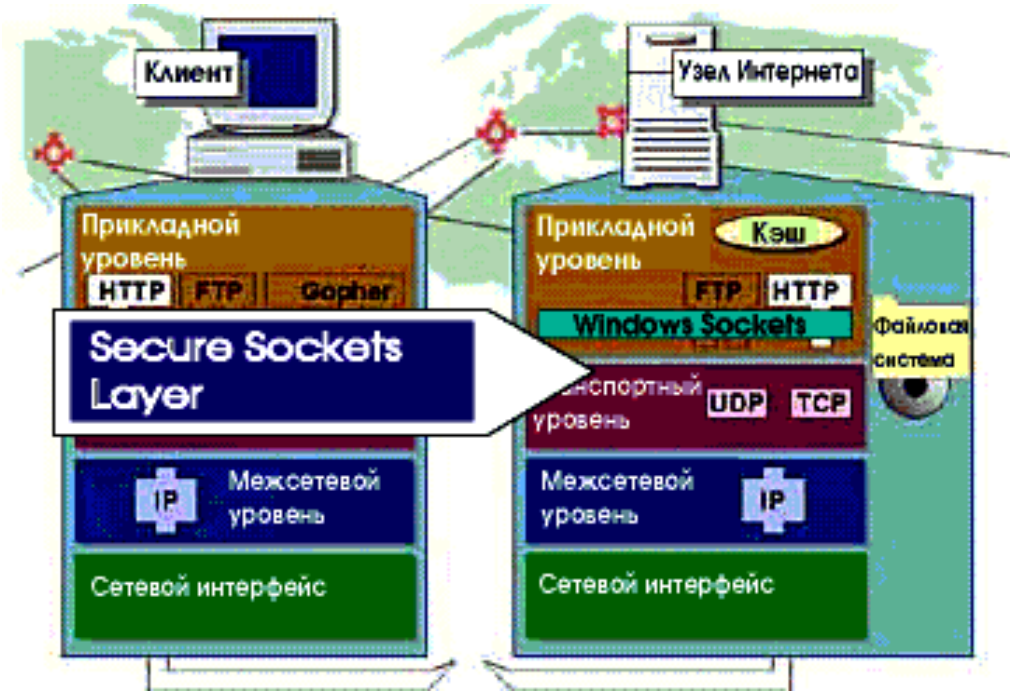
В рамках Internet Information Server SSL функционирует между транспортным и прикладным уровнями модели OSI.

Протокол SSL обеспечивает аутентификацию сервера, шифрование информации и проверку целостности данных.

- Аутентификация гарантирует, что данные передаются именно тому серверу, которому они адресованы, и что сервер обеспечивает защиту данных.
- Шифрование служит гарантией того, что данные не сможет прочесть никто, кроме сервера-адресата.
- Проверка целостности позволяет убедиться, что при передаче данные не были изменены.

Для использования средств протокола SSL на клиенте или сервере необходим цифровой сертификат SSL.

Примечание Основное различие между версиями 2.0 и 3.0 протокола SSL в том, что в версию SSL 3.0 включены средства поддержки клиентских сертификатов.



Цифровые сертификаты SSL

Аутентификация в SSL выполняется с использованием цифрового сертификата, который состоит из следующих полей:

- **Version** — версия;
- **Serial number** — идентификатор сертификата;
- **Signature algorithm ID** — идентификатор алгоритма подписи;
- **Issuer name** — название организации, выдавшей сертификат;
- **Validity period** — срок действия;
- **Subject user name** — имя владельца;
- **Subject public key information** — информация об открытом ключе владельца;
- **Issuer unique ID** — уникальный идентификатор того, кто выдал сертификат;
- **Subject unique identifier** — уникальный идентификатор владельца;
- **Extensions** — расширения;
- **Signature on the above fields** — подпись для перечисленных выше полей. Далее вы узнаете о применении сертификатов SSL для аутентификации.

Аутентификация по сертификатам клиентов

В Internet Information Server Вы не только можете применять SSL для защиты доступа к конкретному виртуальному серверу или папке, но и решить, нужно ли при доступе к этому серверу или папке требовать от клиента предъявления сертификата.

Аутентификация клиента на базе сертификата выполняется при обращении клиента к серверу, использующему протокол SSL и требующему от клиента предоставления сертификата. В этом случае сервер запрашивает у клиента сертификат стандарта X.509, чтобы удостовериться в подлинности пользователя. Только после того, как сервер идентифицирует пользователя, он предоставляет клиенту доступ к ресурсу, заданному соответствующим универсальным идентификатором (Uniform Resource Locator, URL).

Аутентификация с применением сертификата клиента позволяет серверу идентифицировать индивидуальных пользователей и предоставлять им заданные администратором права доступа. Internet Information Server поддерживает аутентификацию клиентов в сеансе защищенного канала посредством сертификатов с открытым ключом. Для использования защищенного канала и сертификата необходимо выполнение перечисленных ниже условий.

- Протокол должен поддерживать сертификацию — то есть обработку соответствующих запросов и ответов — как на клиенте, так и на сервере.
- Клиент обязан уметь проверять сертификаты серверов, запрашивать сертификаты и позволять пользователям предоставлять сертификаты в ответ на запрос. Для этого нужно, чтобы клиент поддерживал хранение сертификатов и управление ими.
- Сервер должен уметь запрашивать сертификаты клиентов, проверять их и связывать со средствами контроля доступа на сервере.

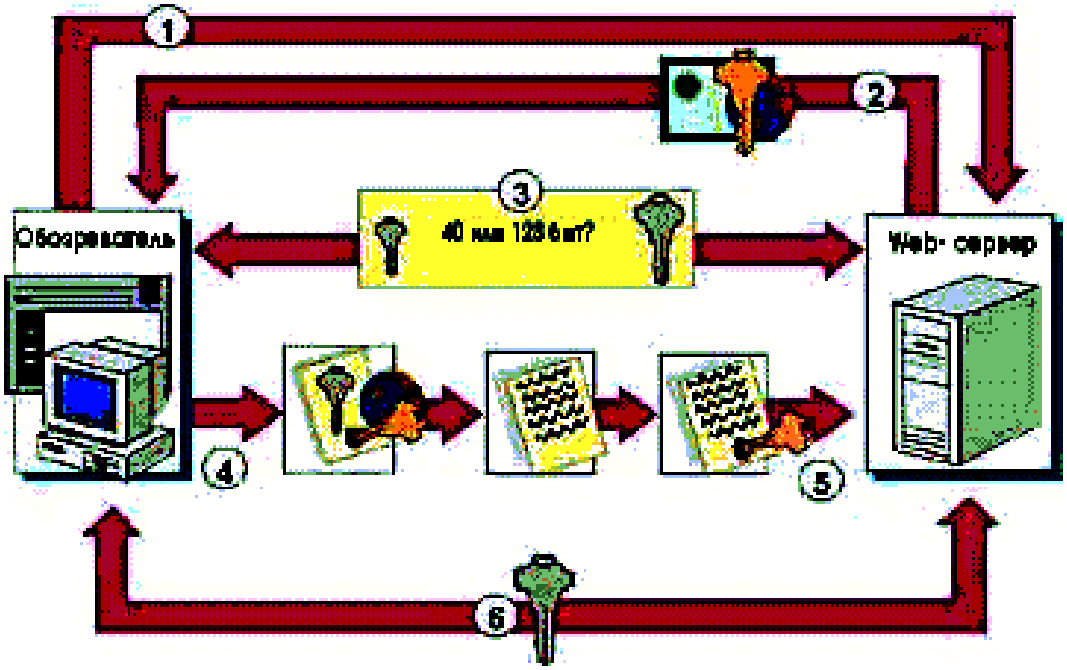
Потокол SSL реализует следующие функции:

- Конфиденциальность соединения. После предварительного диалога ("handshake") определяется секретный ключ, который используется для симметричной криптографии (например, DES или RC4)
- Партнеры идентифицируют друг друга с помощью асимметричных криптографических методов (например, RSA)
- Обеспечение надежности соединения. Пересылка включает в себя контроль целостности сообщений с применением кода аутентификации MAC (Message Autentification Code) и хэш-функций (SHA или MD5).

Создание сеанса SSL

Сеанс SSL, шифрующий все данные, которыми обмениваются клиент и сервер, создается таким образом.

1. Web-обозреватель устанавливает защищенное соединение с Web-сервером.
2. Web-сервер передает обозревателю копию своего сертификата вместе со своим открытым ключом. Сертификат сервера позволяет обозревателю убедиться в подлинности сервера и целостности содержимого узла.
3. Web-обозреватель и сервер начинают обмениваться информацией; при этом определяется длина ключа шифрования, используемого для защиты передаваемой информации (обычно 40 или 128 бит). Действующие в настоящее время ограничения на экспорт технологий шифрования, наложенные правительством США, допускают использование более надежного 128-битного шифрования только в США и Канаде.
4. Web-обозреватель генерирует ключ сеанса и шифрует его открытым ключом сервера. Затем обозреватель передает зашифрованный ключ сеанса Web-серверу.
5. Используя свой личный ключ, сервер дешифрует ключ сеанса и создает защищенный канал.
6. Web-сервер и обозреватель используют ключ сеанса для шифрования и расшифровки передаваемых данных.



Внешние сертифицирующие организации

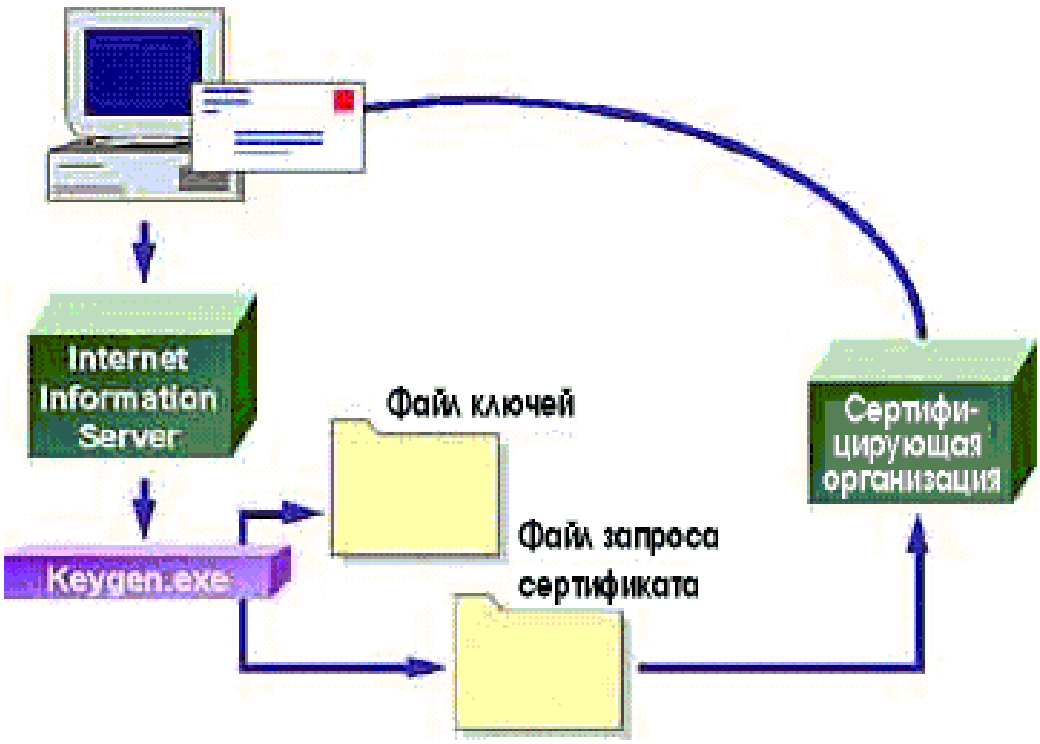
Для того чтобы пользоваться SSL, Вам потребуются соответствующие сертификаты и ключи. На этом занятии Вы узнаете, как получить сертификаты и ключи и как после этого настроить поддержку SSL в Internet Information Server.

Чтобы пользоваться средствами защиты протокола SSL на своем сервере, Вам придется сначала получить для него цифровой сертификат. Затем Вы сможете воспользоваться средствами защиты, предлагаемыми SSL, для защиты своего Web-узла. Чтобы получить цифровой сертификат, нужно сначала зарегистрировать себя или свою организацию в специальном внешнем сертифицирующем органе, который и выдает сертификаты. Полученный сертификат докажет Вашу подлинность другим узлам сети, зарегистрированным в этой же сертифицирующей организации.

Внешние сертифицирующие организации

Чтобы получить цифровой сертификат от внешней сертифицирующей организации, сначала придется создать пару ключей для Вашей системы с помощью утилиты Key Manager. Затем полученный файл запроса сертификата следует отправить по электронной почте сертифицирующей организации. Она зарегистрирует Вас и вышлет Вам подтверждение Вашего цифрового сертификата.

До тех пор пока Вы не отправите запрос сертификата и не получите подтверждения, Вы не можете пользоваться парой ключей, находящихся на Вашем сервере. Зарегистрировавшись в сертифицирующей организации, Вы сможете задействовать средства аутентификации SSL на основе сертификатов клиентов для более надежной защиты Вашего Web-узла.



Чем отличается TLS от SSL?

Протоколы SSL (Secure Socket Layer) и его развитие TLS (Transport Layer Security) предназначены для обеспечения безопасности при передаче конфиденциальной информации через Internet. Протоколы семейства SSL/TLS обеспечивают конфиденциальность, целостность и авторизацию передаваемой информации. Конфиденциальность и целостность передаваемой информации обеспечивается при помощи шифрования сообщений, авторизация осуществляется путем применения цифровых сертификатов.

Протоколы SSL (Secure Socket Layer, протокол защищенных соединений) и TLS (Transport Layer Security, защита на транспортном уровне) предназначены для создания защищенного канала связи. TLS — более современный вариант, его версия 1.0 базируется на версии 3.0 протокола SSL. Однако, несмотря на общие цели и отсутствие принципиальных различий, между SSL и TLS нет совместимости. Основным отличием TLS является его непатентованная технология и возможность обновление более новыми алгоритмами.

TLS состоит из двух протоколов:

- TLS Handshake Protocol (протокол установления соединения) - выполняет двустороннюю аутентификацию и обмен ключевой информацией; предназначен для создания защищенной сессии.
- TLS Record Protocol (протокол записи) - обеспечивает шифрование и контроль целостности передаваемых данных.

SSL и TLS встроены в популярные Интернет-браузеры и наиболее часто используются для защиты обмена по протоколу HTTP.

Конкретизация генерации сеансного ключа

Секретность обеспечивается шифрацией передаваемых сообщений с использованием симметричных сессионных ключей, которыми стороны обмениваются при установлении соединения. Сессионные ключи передаются также в зашифрованном виде, при этом они шифруются с помощью открытых ключей, извлеченных из сертификатов абонентов. Использование для защиты сообщений симметричных ключей связано с тем, что скорость процессов шифрации и дешифрации на основе симметричного ключа существенно выше, чем при использовании несимметричных ключей. Целостность передаваемых сообщений достигается за счет того, что к сообщению (еще до его шифрации сессионным ключом) добавляется дайджест, полученный в результате применения односторонней функции к тексту сообщения.

Сертификаты: какие бывают? Версии?

Взаимная аутентификация обеих сторон в SSL выполняется путем обмена сертификатами при установлении SSL-сессии. SSL поддерживает сертификаты различных сертифицирующих организаций, основанные на стандарте X.509, а также стандарты инфраструктуры публичных ключей PKI (Public Key Infrastructure), с помощью которой организуется выдача и проверка подлинности сертификатов.
Спецификации PKIX основаны на двух группах стандартов: X.509 ITU-T (Международный комитет по телекоммуникациям) и PKCS (Public Key Cryptography Standards) firmy RSA Data Security.

Стандарт X.509 ITU-T является фундаментальным стандартом, лежащим в основе всех остальных, используемых в ИОК. Основное его назначение - определение формата электронного сертификата и списков отозванных сертификатов.

Cryptographic Service Provider(CSP)
UniCert 3.5 фирмы Baltimore Technologies,
Entrust 5.01 фирмы Entrust Technologies,
Keon 5.5 фирмы RSA Security и OnSite 4.51 фирмы VeriSign.

Хотеться подчеркнуть что внедрения PKI(X.500) в коммерческих структурах не находит большего применения из-за его иерархической модели. Иерархическая модель обозначений соответствует военным и гос. структурам, но не работает для бизнеса.

Резюме

Протокол SSL позволяет серверу и клиенту безопасно обмениваться конфиденциальными данными по Интернету. SSL обеспечивает защиту передаваемых данных с помощью аутентификации сервера, шифрования данных и проверки их целостности. Аутентификация в SSL основана на использовании цифровых сертификатов. Аутентификация с помощью сертификата клиента позволяет серверу идентифицировать и авторизовать индивидуальных пользователей. Вы можете получить цифровые сертификаты от внешних сертифицирующих органов — например, от компании VeriSign. Microsoft Certificate Server предоставляет администратору полный контроль над выдачей,

обновлением и отзывом сертификатов SSL, избавляя от необходимости обращаться ко внешним организациям для сертификации клиентов Вашего узла.

В работе использовались материалы с сайта: **http://www.rsa.com/ http://www.citforum.ru**
статья Э.Сергеева "Протокол SSL и защита информации в системе RS-Portal"