Технологии защиты от несанкционированного доступа

Дубинин Евгений
Жогот Семен
Группа И-2-13

Технология SSL

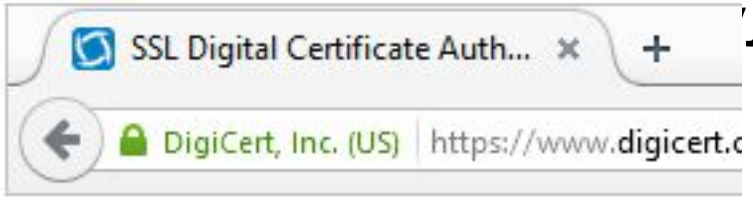
- В настоящее время, случаи онлайн кражи персональных данных становятся все более популярными. Важным моментом является создание доверенной среды, где потенциальные клиенты чувствовали бы себя уверенно при совершении банковских операций и покупок в интернете. SSL- является широко распространенным протоколом безопасности, используемым сегодня для создания зашифрованного канала связи между сервером и клиентом.

Технология SSL

- По существу, это протокол, который позволяет надежно передавать конфиденциальную информацию, обеспечивая безопасность работы в интернете или внутренней сети. Технически SSL является прозрачным протоколом, который требует небольшого взаимодействия с конечным пользователем при создании безопасного сеанса.

Технология SSL

- В случае браузера, например, пользователи предупреждаются о том, что они находятся на безопасном сайте (наличии SSL), когда отображается замок, а в случае (Extended Validation SSL) в адресной строке появится замок и зеленая полоска (Green Bar). Адреса начинаются с "HTTPS: //" - и соединение происходит на порт 443 по умолчанию. В приведенных ниже изображениях, вы можете увидеть лярных браузеро



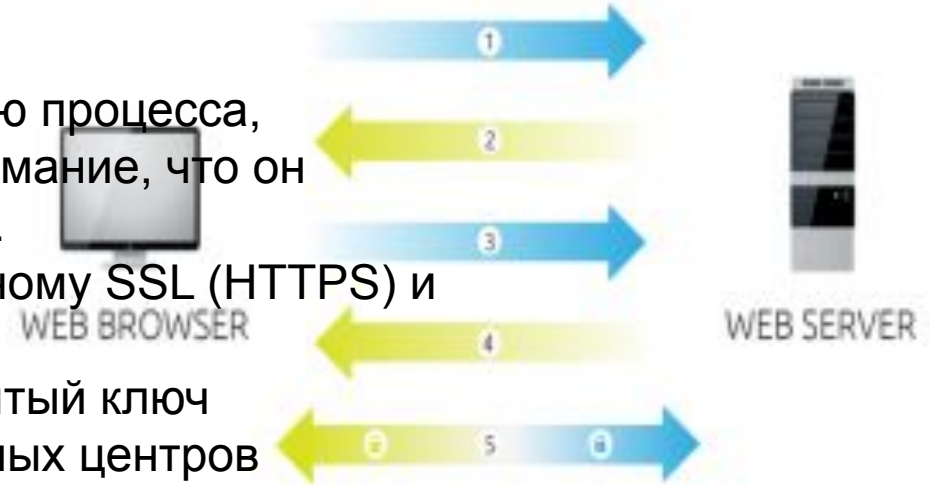
Firefox

Opera

Процесс создания защищенного соединения?

Процесс создания защищенного соединения?

Браузер и веб-сервер устанавливают SSL соединение с помощью процесса, называемого "SSL-диалог" (смотрите схему ниже). Обратите внимание, что он является невидимым для пользователя и происходит мгновенно.



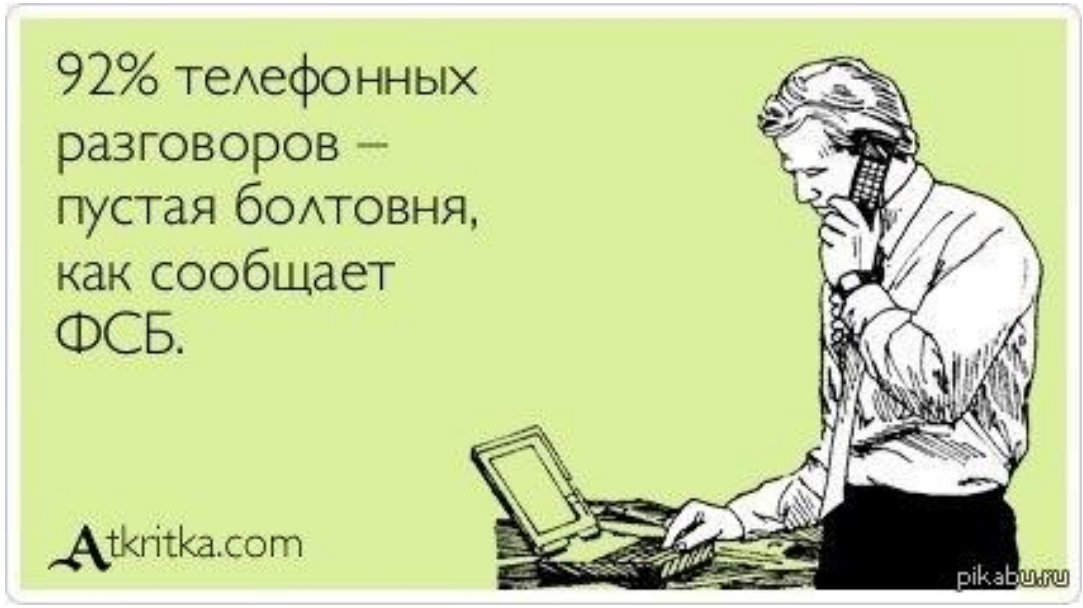
1. Браузер подключается к веб-серверу (веб-сайту), обеспеченному SSL (HTTPS) и запрашивает у сервера идентифицировать себя.
2. Сервер посылает копию своего SSL сертификата и свой открытый ключ
3. Браузер проверяет корневой сертификат со списком доверенных центров сертификации. Если браузер доверяет сертификату то он создает, используя открытый ключ сервера и отправляет обратно зашифрованный симметричный ключ сеанса.
4. Сервер расшифровывает симметричный ключ сеанса, используя свой закрытый ключ и отправляет обратно подтверждение, зашифрованное с помощью ключа сеанса, таким образом создается шифрованный канал связи.
5. Сервер и браузер шифруют все передаваемые данные с помощью временного симметричного ключа.

Технология TLS

- **TLS** (безопасность транспортного уровня), как и его предшественник SSL —криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет. TLS и SSL используют асимметричную криптографиюдля аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.
- Данный протокол широко используется в приложениях, работающих с сетью Интернет, таких как веб-браузеры, работа с электронной почтой, обмен мгновенными сообщениями и IP-телефония (VoIP).

Технология TLS

- TLS даёт возможность клиент-серверным приложениям осуществлять связь в сети таким образом, чтобы предотвратить прослушивание и несанкционированный доступ.



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;
- 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 отзван ли серверный сертификат, связавшись с сервисом доверенного удостоверяющего центра;
- для шифрования сессии используется сеансовый ключ. Получение общего секретного сеансового ключа клиентом и сервером проводится по протоколу Диффи-Хеллмана.

- На этом заканчивается процедура подтверждения связи. Между клиентом и сервером установлено безопасное соединение, данные, передаваемые по нему, шифруются и расшифровываются с использованием симметричной криптосистемы до тех пор, пока соединение не будет завершено.
- При возникновении проблем на некоторых из вышеуказанных шагов подтверждение связи может завершиться с ошибкой, а безопасное соединение не будет установлено.

Технология IPsec

- **IPsec** (сокращение от **IP Security**) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет.

Архитектура IPsec

Построение защищённого канала связи может быть реализовано на разных уровнях модели OSI. Так, например, популярный SSL-протокол работает на уровне представления, а PPTP — на сеансовом.

Уровни OSI	Протокол защищённого канала
Прикладной уровень	S/MIME
Уровень представления	SSL, TLS
Сеансовый уровень	PPTP
Транспортный уровень	AH, ESP
Сетевой уровень	IPsec
Канальный уровень	
Физический уровень	

В работе протоколов IPsec можно выделить пять этапов:

- Первый этап начинается с создания на каждом узле, поддерживающим стандарт IPsec, политики безопасности. На этом этапе определяется, какой трафик подлежит шифрованию, какие функции и алгоритмы могут быть использованы.
- Второй этап является по сути первой фазой IKE. Её цель — организовать безопасный канал между сторонами для второй фазы IKE. На втором этапе выполняются:
  - Аутентификация и защита идентификационной информации узлов
  - Проверка соответствий политик IKE SA узлов для безопасного обмена ключами
  - Обмен Диффи-Хеллмана, в результате которого у каждого узла будет общий секретный ключ
  - Создание безопасного канала для второй фазы IKE
- Третий этап является второй фазой IKE. Его задачей является создание IPsec-туннеля. На третьем этапе выполняются следующие функции:
  - Согласуются параметры IPsec SA по защищаемому IKE SA каналу, созданному в первой фазе IKE
  - Устанавливается IPsec SA
  - Периодически осуществляется пересмотр IPsec SA, чтобы убедиться в её безопасности
  - (Опционально) выполняется дополнительный обмен Диффи-Хеллмана
- Рабочий этап. После создания IPsec SA начинается обмен информацией между узлами через IPsec-туннель, используются протоколы и параметры, установленные в SA.
- Прекращают действовать текущие IPsec SA. Это происходит при их удалении или при истечении времени жизни (определенное в SA в байтах информации, передаваемой через канал, или в секундах), значение которого содержится в SAD на каждом узле. Если требуется продолжить передачу, запускается фаза два IKE (если требуется, то и первая фаза) и далее создаются новые IPsec SA. Процесс создания новых SA может происходить и до завершения действия текущих, если требуется непрерывная передача данных.

Технология RPC

- RPC интегрирован с компонентами поддержки защиты (security support providers, SSP), что позволяет клиентам и серверам RPC использовать аутентификацию и шифрование при коммуникационной связи. Когда серверу RPC требуется защищенное соединение, он сообщает библиотеке RPC периода выполнения, какую службу аутентификации следует добавить в список доступных служб аутентификации. А когда клиенту нужно использовать защищенное соединение, он выполняет привязку к серверу.

- Во время привязки к серверу клиент должен указать библиотеке RPC службу аутентификации и нужный *уровень аутентификации*. Различные уровни аутентификации обеспечивают подключение к серверу только авторизованных клиентов, проверку каждого сообщения, получаемого сервером (на предмет того, послано ли оно авторизованным клиентом), контроль за целостностью RPC-сообщений и даже шифрование данных RPC-сообщений. Чем выше уровень аутентификации, тем больше требуется обработки. Клиент также может указывать *имя участника безопасности* (principal name) для сервера. *Участник безопасности* (principal) — это сущность, распознаваемая системой защиты RPC Сервер должен зарегистрироваться в SSP под именем участника безопасности, специфичным для SSP.

- SSP берет на себя все, что связано с аутентификацией и шифрованием при коммуникационной связи, не только для RPC, но и для Winsock. В Windows несколько встроенных SSP, в том числе Kerberos SSP, реализующий аутентификацию Kerberos v5, SChannel (Secure Channel), реализующий Secure Sockets Layer (SSL), и протоколы TLS (Transport Layer Security). Если SSP не указан, программное обеспечение RPC использует встроенные средства защиты нижележащего транспорта. Одни транспорты, в частности именованные каналы и локальный RPC, имеют такие средства защиты, а другие, например TCP, — нет. В последнем случае RPC при отсутствии указанного SSP выдает небезопасные вызовы.

Технология DCOM

- **DCOM** - программная архитектура, разработанная компанией Microsoft для распределения приложений между несколькими компьютерами в сети. Программный компонент на одной из машин может использовать DCOM для передачи сообщения (его называют удаленным вызовом процедуры) к компоненту на другой машине. DCOM автоматически устанавливает соединение, передает сообщение и возвращает ответ удаленного компонента.

- COM и DCOM - технологии, обеспечивающие взаимодействие между компонентами приложения и позволяющие развертывать распределенное приложение на платформе Windows. COM является моделью программирования на основе объектов, которая упрощает взаимодействие различных приложений и компонентов, а DCOM - это своего рода "клей", связывающий воедино разнообразные технологии, применяемые в распределенных приложениях. DCOM дает возможность двум или нескольким компонентам легко взаимодействовать друг с другом независимо от того, когда и на каком языке программирования они были написаны, а также где именно они находятся и в какой операционной системе работают

- Преимуществом DCOM является значительная простота использования. Если программисты пишут свои Windows-приложения с помощью ActiveX (предлагаемого Microsoft способа организации программных компонентов), то операционная система будет автоматически устанавливать необходимые соединения и перенаправлять трафик между компонентами, независимо от того, размещаются ли компоненты на той же машине или нет.

- Способность DCOM связывать компоненты позволила Microsoft наделить Windows рядом важных дополнительных возможностей, в частности, реализовать сервер Microsoft Transaction Server, отвечающий за выполнения транзакций баз данных через Internet. Новая же версия COM+ еще больше упростит программирование распределенных приложений, в частности, благодаря таким компонентам, как базы данных, размещаемые в оперативной памяти.

- Однако у DCOM есть ряд недостатков. Это решение до сих пор ориентировано исключительно на системы Microsoft. DCOM изначально создавалась под Windows. Хорошо известно, что Microsoft заключила соглашение с компанией Software AG, предмет которого - перенос DCOM на другие платформы.