Россия, Санкт-Петербург, ВКА имени А.Ф. Можайского
ктн Пилькевич С.В., Киселев С.С.

Протокол SSL/TLS как основа технологии VPN.

Введение

Современный этап развития общества напрямую связан с ростом ценности информации, циркулирующей в цифровых системах связи и передачи данных. Наиболее действенным средством обеспечения конфиденциальности, целостности и аутентичности, передаваемых по каналам связи данных, являются криптографические протоколы и построенные на их основе виртуальные частные сети (VPN от английского Virtual Private Network).

Термином VPN принято обозначать технологию, позволяющую обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрованию, аутентификации, инфраструктуры открытых ключей, средствам для защиты от повторов и изменения передаваемых по логической сети сообщений) [4].

В настоящее время существует большое количество различных реализаций технологии VPN, к наиболее распространенным среди них следует отнести следующие: IPSec, PPTP, PPPoE, L2TP и OpenVPN.

В настоящей статье более пристальное внимание будет уделено, в частности, OpenVPN - реализация технологии VPN с открытым исходным кодом для создания зашифрованных каналов типа «точка-точка» или «сервер-клиенты» между компьютерами. Для обеспечения безопасности управляющего канала и потока данных, OpenVPN использует библиотеку OpenSSL. Благодаря этому задействуется весь набор криптографических алгоритмов, доступных в данной библиотеке и, как следствие, данная реализация виртуальной частной сети базируется на протоколах SSL и TLS.

Протокол SSL (и его более новая модификация - TLS) предназначен для решения традиционных задач обеспечения защиты информационного взаимодействия:

- клиент и сервер должны быть уверены в достоверности стороны, с которой осуществляют обмен информацией;

- после установления соединения между сервером и клиентом весь информационный поток между ними должен быть защищен от несанкционированного доступа;

- при обмене информацией стороны информационного взаимодействия должны быть уверены в отсутствии случайных или умышленных искажений.

Для уяснения способов решения этих задач, необходимо рассмотреть основные термины, которые используются в SSL. В первую очередь это инфраструктура открытых ключей, шифрование и аутентификация.

Инфраструктура открытых ключей

Общими целями современных архитектур безопасности являются защита и распространение информации в распределенной среде, где пользователи, ресурсы и посредники разделены во времени и пространстве. Инфраструктура открытых ключей (PKI) обеспечивает сервисы, необходимые для непрерывного управления ключами в распределенной системе, связывает открытые ключи с владельцами соответствующих секретных ключей и позволяет пользователям проверять подлинность этих связей [8].

Инфраструктура открытых ключей обеспечивает решение следующих задач:

1) лицо или процесс, идентифицируемый как отправитель электронного сообщения или документа, действительно является инициатором отправления;

2) лицо или процесс, выступающий получателем электронного сообщения или документа, действительно является тем получателем, которого имел в виду отправитель;

3) целостность передаваемой информации не нарушена.

Цель PKI состоит в управлении ключами и сертификатами. PKI позволяет использовать сервисы шифрования и выработки цифровой подписи согласованно с широким кругом приложений, функционирующих в среде открытых ключей [8].

Шифрование

Основным способом обеспечения конфиденциальности информации является шифрование - способ преобразования открытой информации в закрытую и обратно. Шифрование объединяет в себе термины *зашифрование* и *расшифрование*.

Зашифрование - процесс преобразования открытого сообщения в шифрованное сообщение с помощью инъективной функции, зависящей от ключа. Зашифрование должно нарушать лингвистические и статистические связи в исходном открытом сообщении. Функция шифрования и функция расшифрования при любом значении ключа должны допускать простую техническую реализацию. При неизвестном секретном ключе для каждого открытого сообщения, или хотя бы близкому к нему, должна с заданной надежностью характеризоваться высокой сложностью (теоретико-информационной, алгоритмической и вычислительной) [9].

Аутентификация

Аутентификация - установление (то есть проверка и подтверждение) подлинности различных аспектов информационного взаимодействия: содержания и источника передаваемых сообщении, сеанса связи, времени взаимодействия [9].

Криптографический протокол SSL/TLS

Протокол SSL (Secure Socket Layer)- криптографический протокол, обеспечивающий безопасную передачу данных по сети [3], позволяет серверу и клиенту перед началом информационного взаимодействия аутентифицировать друг друга, согласовать набор алгоритмов шифрования и сформировать общие криптографические ключи.

В SSL используется самые разнообразные методы криптографического преобразования данных. Аутентификация сообщений осуществляется путем использования электронной цифровой подписи [2]. Контроль целостности передаваемых блоков данных производится за счет использования кодов аутентификации сообщений, вычисляемых с помощью хэш-функций [1]. Распределение ключевой информации производится на основе методов асимметричной криптографии. Конфиденциальность информации, обеспечивается путем шифрования потока данных на сформированном общем сессионном ключе с использованием симметричных криптографических алгоритмов.

Протокол SSL включает четыре этапа взаимодействия сторон информационного обмена [6]:

1) согласование параметров SSL-сессии;

2) аутентификация посредством сертификатов;

3) обмен ключами;

4) криптографическая защита потока данных.

Рассмотрим каждый из перечисленных этапов более подробно.

Процедуру согласования параметров SSL-сессии зачастую называют протоколом рукопожатия или «handshake». В процессе установления связи между клиентом и сервером осуществляется выбор набора криптографических алгоритмов, которые будут использованы в рамках текущей сессии [2].

Выбор варианта протокола аутентификации зависит от настроек программного (и/или аппаратного) обеспечения - сервера информационного обмена.

Для протокола SSL существует три варианта аутентификации [1]:

- односторонняя аутентификация (производится только сервером);
- взаимная аутентификация (производится и клиентом, и сервером);
- без аутентификации сторон.

Обмен ключами и формирование общего сеансового ключа шифрования (TEK – Traffic Encryption Key) представляет собой итерационную процедуру в основе которой лежит один из широко известных протоколов обмена ключами – Диффи-Хеллмана, Эль-Гамаля, Шнорра и др., однако гораздо более сложная и включающая в себя целый ряд операций с промежуточными ключами, начиная от персональных идентификаторов и ключей авторизации (AK - authorization key) и заканчивая ключами шифрования ключа (KEK - Key encryption key), используемыми для шифрования и распределения ключей TEK.

Заключительным этапом защищенного клиент-серверного взаимодействия является криптографическая защита потока данных. Клиент и сервер производят обмен информацией друг с другом. Все данные зашифрованы, посредством согласованного на предыдущих этапах набора криптографических алгоритмов и ключевой информации. Информационные сообщения прикладного уровня делятся на блоки, для каждого блока вычисляется код аутентификации сообщений. Блоки шифруются с использованием симметричных криптографических алгоритмов и отправляются приемной стороне. Приемная сторона производит обратные действия: расшифрование, проверку кода аутентификации сообщения, сборку сообщений, передачу на прикладной уровень.

Заключение

В данной статье была рассмотрена одна из основных проблем в современных информационно-вычислительных системах - защита данных в компьютерных сетях и Интернете. Для решения этой проблемы наиболее оптимальным является использование криптографического протокола SSL/TLS. Дальнейшее его изучение требуется для подтверждения правильной реализации протокола в конечных программных продуктах.

В статье раскрываются основные термины, используемые в протоколе: инфраструктура открытых ключей, шифрование и аутентификация. Так же раскрывается цель и функции криптографического протокола SSL/TLS.

Список используемой литературы:

1) RFC 2246 – The TLS Protocol Version 1.0.
2) RFC 5246 – The Transport Layer Security (TLS) Protocol Version 1.2
3) Alan O. Freier, Philip Karlton, and Paul C. Kocher. INTERNET–DRAFT The SSL Protocol Version 3.0. – 1996
4) http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00
5) Kipp E. B. Hickman. SSL 2.0 Protocol Specification. – 1996
6) http://www.mozilla.org/projects/security/pki/nss/ssl/draft02.html
7) Microsoft Corporation – «TLS/SSL Works». – 2009

8) http://technet.microsoft.com/en–us/library/cc783349(WS.10).aspx
9) SSLFail.com SSLv3 Traces. – 2009
10) http://www.sslfail.com/2009/01/sslv3–traces–part–1/
11) Олифер В.Г. Олифер Н.А. Компьютерные сети: Принципы, технологии, протоколы. – Питер. – 2009. – 958с.
12) Горбатов В.С. Полянская О.Ю. Основы технологии PKI. - Москва - Горячая Линия – Телеком – 2004 г. - 248с.
13) Погорелов Б.А. Сачкова В.Н. Словарь криптографических терминов. - Москва - 2006 г. – МЦМНО – 88с.