Эссе по курсу «Защита информации», кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ), http://www.re.mipt.ru/infsec

Сравнение протоколов IPSec и SSL
A Technical Comparison of IPSec and SSL

Выполнил студент 211 группы
Шабашов Евгений

2006 год

Введение

Защита данных в сетях довольна трудная задача. IP сети восприимчивы к большому числу угроз, например, получение доступа обманным путем (т.н. spoofing), потеря секретности, потеря целостности данных, контроль соединения и отказ от обслуживания (denial-of-service). Цель средств обеспечивающих безопасноть данных в сети - это *конфиденциальность передаваемых данных*, их *целостность* и *аутентификация*.

Конфиденциальность предполагает защиту данных от несанкционированного прослушивания злоумышленником. Наиболее распространенным способом такой защиты является шифрование. Реализация алгоритмов шифрования достаточно проста, несмотря на всю сложность математических алгоритмов, которые они используют. Трудность же возникает только в управлении ключами защиты. Использование шифрования снижает производительность системы. Решением проблемы может стать использование аппаратно реализованных средств шифрования, тем самым мы освобождаем защитное устройство от дополнительной нагрузки.

Целостность подразумевает идентичность отправленных и полученных данных. Для решения такого рода задач используется алгоритмы хеширования. На основе исходного сообщения вычисляется значение хеш-функции, (это может быть или цифровая подпись или хэш с фиксированной длиной.) приемная сторона производит теже операции и сравнивает полученное и вычисленное значение. На основани этого делается вывод о целостности полученного сообщения.

Механизм *аутентификации* позволяет определить, достоверность того, что человек, общающийся с вами действительно тот, за кого себя выдает.

Все эти свойства должны быть присущи любому протоколу безопасности, но они могут быть реализованы в каждом из протоколов в разной форме.

На данный момент неаиболее надежными считаются протоколы IPSec (IP Security) и SSL (Secure Socket Layer). Каждая из технологий имеет как недостатки, так и преимущества. Я попытаюсь отразить их в докладе.

IP Security

IPSec – это набор протоколов, решающих проблемы по шифрованию данных, их целостности и аутентификации. IPSec работает на сетевом уровне. Таким образом, защита данных будет прозрачна для сетевых приложений.

Для протокола IPSec были разработаны два вида заголовков аутентификационный заголовок (Authentication Header) и заголовок безопасного скрытия данных (Encapsulating Security Payload). Каждый из заголовков призван решать задачи связанные с безопасностью передаваемых данных.

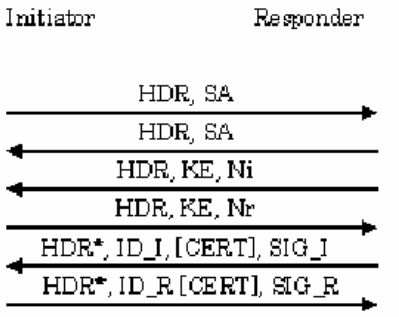
Аутентификационный заголовок (AH) призван обеспечивать целостность данных, аутентификацию и защиту от воспроизведения. Он не обеспечивает секретности - передаваемые данные не зашифрованы. Он располагается между основным заголовком IP-пакета и полем данных.

Для шифрования передаваемых данных используется *протокол ESP*. Главной его задачей является обеспечение конфеденциальности данных, с этой целью могут применяться различные алгоритмы шифрования TCP-пакета. После шифрования к пакету дописывается заголовок ESP, который содержит информацию необходимую для расшифрования. Может также использоваться с дополнительной полем аутентификации, что обеспечивает установление подлинности.

Для работы этих протоколов необходима инфраструктура, которая бы занималась согласованием алгоритмов шифрования и характеристик ключей, распределением ключей между общающимися сторонами. Для этих целей была разработана группа протоколов Internet Key Exchange (IKE). На нее так же возложены задачи по контролю выполнения соглашений.

Установление IPSec соединения проходит в две фазы: Phase 1 (ISAKMP SA) и Phase 2 (IPSec SA)
Первая фаза может проходить в одном из двух режимов.

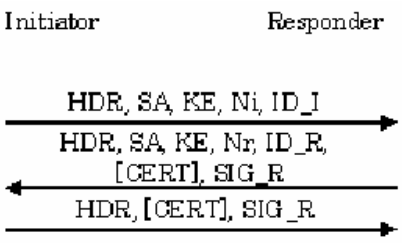
Основной режим



В ходе первой передачи сообщений стороны договариваются о базовых алгоритмах и методах хеширования. Во второй осуществляется обмен открытыми ключами Диффи — Хеллмана и случайными числами, которые подписываются принимающими сторонами и отправляются обратно для идентификации. На третьем шаге по полученным подписанным значениям проверяется подлинность сторон.

Итого для установления требуется 6 циклов обмена сообщениями.

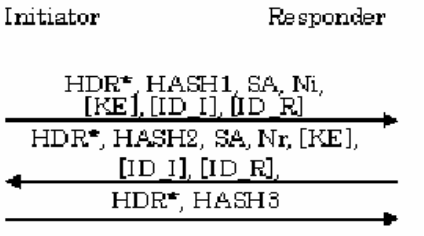
Агрессивный режим



Данный режим более производителен, но менее безопасный, так как данные необходимые для идентификации сторон передаются в незащищенном виде.

Но количество циклов уменьшено до 3х.

Вторая фаза может проходить только в «*быстром режиме*» (Quick mode). В ходе нее происходит согласование параметров SA (Security Association) и генерация новых ключей. В быстром режиме все передачи осуществляются по защищенному «туннелю».



Его реализация во многом похожа на реализацию агрессивного режима: один цикл включает в себя передачу трех пакетов.

Secure Socket Layer

SSL (Secure Socket Layer) протокол уровня приложений, в основном используется для защищенного обмена информацией между удаленными приложениями (по большей части это обращение к Web- серверам).

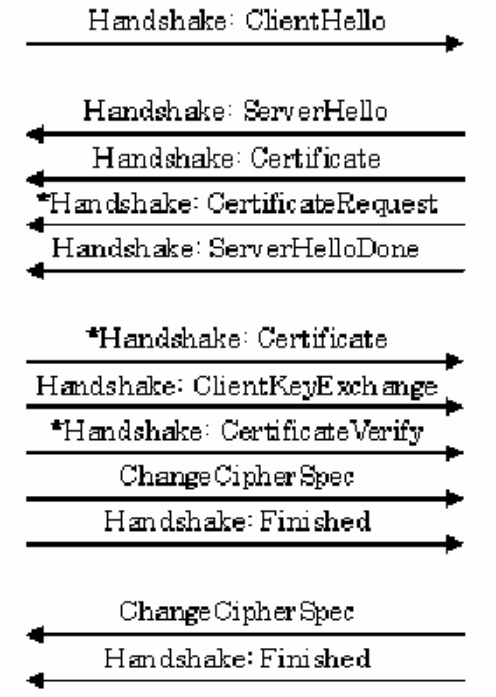
Преимущество протокола SSL в том, что он имеет два уровня: протокол записей (SSL Record Protocol) и протокол диалога (SSL Handshake Protocol). В качестве несущей среды может выбираться протокол TCP, который совместно с SSL Record Protocol, образует так называемое ядро SSL, поверх которого могут накладываться другие протоколы.

SSL Handshake Protocol используется для аутентификации сторон, а так же для согласования определенного алгоритма шифрования и обмена ключами.

Одним из преимуществ является его независимость от программ и платформ, на которых он используется.

SSL вступает в силу, когда вы пытаетесь зайти на адрес начинающийся с https. По умолчанию SSL использует 443 порт.

Схема аутентификации:



В начале общения клиент посылает сообщения формата “Hello”, на которое сервер отвечает аналогичным приветственным сообщением. Эти сообщения содержат данные для открытия секретного канала (версия протокола, идентификатор сессии, способ шифрования, метод компрессии и сгенерированное число). Далее сервер отсылает свой сертификат. И после окончательного уточнения всех параметров стороны могут приступить к передаче зашифрованной информации.

Этот процесс может занять довольно длительное время.

Техническое сравнение

1 Архитектура

Основное различие состоит в том, что IPSec - это протокол сетевого уровня, в то время как SSL - это протокол уровня приложений. IPSec одинаково обращается с пакетами протоколов более высокого уровня, то есть аутентифицируются и шифруются, не обращая внимания на их содержание**.**

Для работы SSL необходим надежный транспортный протокол (например, TCP).

Надежность IPSec еще гарантируется тем, что информация о порте, с которым установлено соединение так же недоступна для злоумышленника.

IPSec поддерживает три вида установления соединения

- Gateway-to- Gateway
- Gateway-to-Host
- Host-to-Host

SSL поддерживает только соединение между двумя host’ами или клиентом и сервером.

Так как IPSec это протокол сетевого уровня, то его реализация легко может быть встроена в ядро системы или как отдельное устройство.

2 Аутентификации

В случае IPSec аутентификация всегда двусторонняя, а для SSL она быть как взаимной, так и односторонней (или отсутствовать вообще).

Table 3: IPSec Authentication Method

Authentication Method	Authentication Algorithm
Mutual Authentication	PSK
	RSA/DSA Digital Signature
	RSA Public Key
	KINK

Table 4: SSL Authentication Method

Authentication Method	Authentication Algorithm
Server Authentication	RSA (Challenge/Response)
	DSA Digital Signature
Client Authentication	RSA/DSA Digital Signature
Anonymous	none

IPSec поддерживает цифровую подпись и использование Secret Key Algorithm, в то время как SSL поддерживает только цифровую подпись. И IPsec и SSL могут использовать PKI. Премущество IPSec в том, что для малых систем, можно вместо PKI, а использовать preshared keys, что заметно упрощает задачу. Методы, которые используются в SSL, идеально подходят для установления защищенного соединения между сервером и клиентом.

Основное различие между способами аутентификации опять же заключается в том, что IPSec функционирует на сетевом уровне. Таким образом, есть возможность прослеживать адрес получателя и источника с тем же успехом и аутентификацию более высоких уровней. SSL же имеет доступ только к информации транспортного уровня и выше.

3. Способ соединения.

IPSec поддерживает два режима работы.

- *Туннельный режим* (ESP) Устанавливается туннель между оконечными точками(Gateway-to-Gateway, Gateway-to-Host, Host-to-Host). Исходный IP пакет шифруется (включая заголовок), потом к нему добавляется заголовок ESP
- *Транспортный режим* (ESP) (Это соединение типа Host-to-Host.) В данном режиме шифруются только данные.

В случае SSL ситуация обратная. SSL поддерживает единственное соединение за одну сессию. Каждая сессия независима, но производительность может падать с ростом числа сессий. Для каждого соединения шифровальный ключ уникален, что повышает безопасность соединения.

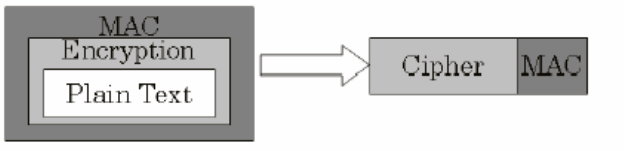
Туннельный режим используется в построении VPN. Два оконечных маршрутизатора шифруют данные таким образом, что от злоумышленника скрываются не только передаваемые данные, но так же источник и пункт назначения. Несколько пользователей одновременно могут использовать один и тот же туннель между двумя оконечными точками.

SSL же не поддерживает туннелирования, т.е. если захотеть устанавливать VPN между двумя подсетями, то нужен некоторый "внешний" способ/протокол туннелирования.

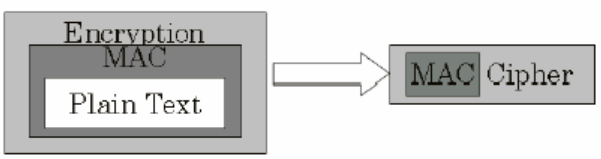
4.Шифрование.

И IPSec и SSL могут реализовывать большое количество криптографических алгоритмов. Различие состоит в последовательности выполняемых действий.

IPSec сначала шифрует данные, а потом добавляет к ним MAC. Если бы в середине транзакции исправленные данные были добавлены, IPSec проверил бы MAC перед выполнения действий по расшифрованию.



В случае SSL сначала создается MAC для исходных данных, потом проходит шифрование. Таким образом, сначала проходит расшифрование,а потом проверка MAC. Это может привести к дополнительной нагрузке процессора, в случае измененных пакетов.



5 Размер служебной информации.

Protocol	Mode	Byte Size
IPSec Tunnel Mode	ESP	32
	ESP and AH	44
IPSec Transport Mode	ESP	36
	ESP and AH	48
SSL	HMAC-MD5	21
	HMAC-SHA-1	25

Один из недостатков IPSec большой обьем дополнительной информации добавляемой к исходному пакету. В случае SSL этот размер значительно меньше. В таблице представлены сравнительные характеристики.

6. Использование алгоритмов сжатия.

Для сжатия IPSec использует протокол IPComp. SSL в меньшей мере использует сжатие, и только OpenSSL поддерживает сжатие в полной мере.

В случае IPSec использование алгоритмов сжатия может приводить к разным результатам при использованиии их в разных условиях: производительность может как увеличиваться, так и уменьшаться. Результат зависит от соотношения скоростей шифрования, сжатия и скорорости передачи данных. Большинство алгоритмов шифрования работают быстрее алгоритмов сжатия. Следовательно, это будет приводить к замедлению работы. Но в случае низкой скорости передачи, использование сжатия заметно увеличит производительность.

Заключение.

Я попытался представить сходства и различия между протоколами IPSec и SSL. Каждый из них имеет уникальные свойства и выбор какого-то из них должен основываться на требованиях, предьявляемых к безоапсности соединения. Основные моменты приведены в таблице.

Function	IPSec	SSL
Configuration	hard	easy
Client Authentication	must	option
Pre-Shared Key	yes	no
Interoperability Problem	yes	no
TCP Application Support	all	some
UDP support	yes	no
Throughput Rate	high	high
Compression Support	yes	OpenSSL only
Handshake Time	slow	fast

Основное преимущество IPSec является то, что он работает на более низком уровне модели OSI, что позволяет ему решать более сложные задачи. И пока SSL удается на равных конкурировать с IPSec, но с появлением и окончательной стандартизацией IPv6 ситуция должна измениться.

Список используемой литературы.

1. AbdelNasir Alshamsi, Takamichi "A Technical Comparison of IPSec and SSL" Saito Tokyo University of Technology , 2003 (http://eprint.iacr.org/2004/314.pdf)
2. http://www.galaxy.com.ua/news/computers/comp0502.htm
3. *Павел Иванов* Сети #02/2000 (http://www.osp.ru/text/302/140914.html)
4. http://www.homeport.org/~adam/ssl.html
5. http://www.nestor.minsk.by/sr/2003/06/30613.html
6. http://inssl.com/content/view/13/26/