ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

«БЕЗОПАСНОСТЬ СЕТЕВОГО УРОВНЯ В IP-СЕТЯХ»

Калинин Михаил
Соавтор:
Тутова Наталья Владимировна
ВУЗ: *МТУСИ*

Ключевые слова: безопасность на сетевом уровне, безопасные IP протоколы – IPSec**,** Протокол безопасности инкапсуляции (ESP), Ассоциация безопасности (SA), Индекс параметров безопасности (SPI), база данных политики безопасности

Key words: network-level security, secure IP protocols - IPSec, Encapsulation Security Protocol (ESP), Security Association (SA), Security Settings Index (SPI), security policy database

Введение

Средства управления безопасностью сетевого уровня часто используются для защиты связи, особенно через общие сети, такие как Интернет, потому что они могут обеспечить защиту для многих приложений одновременно, не изменяя их.

Для обеспечения безопасности сети были разработаны многие протоколы безопасности в режиме реального времени, обеспечивающие основные принципы безопасности, такие как конфиденциальность, аутентификация источника, целостность сообщений и отказ от авторства.

Большинство из этих протоколов оставались сфокусированными на более высоких уровнях стека протоколов OSI, чтобы компенсировать внутреннее отсутствие безопасности в стандартном интернет-протоколе. Несмотря на свою ценность, эти методы не могут быть легко обобщены для использования с любым приложением.

Например, SSL разработан специально для защиты приложений, таких как HTTP или FTP. Но есть несколько других приложений, которые также нуждаются в безопасной связи.

Эта необходимость привела к разработке решения безопасности на уровне IP, чтобы все протоколы более высокого уровня могли использовать его в своих интересах. В 1992 году Инженерная рабочая группа по Интернету (IETF) начала определять стандарт «IPsec» [1].

В данной работе проведен анализ того, что безопасность на сетевом уровне происходит благодаря популярному набору протоколов IPsec.

Безопасность на сетевом уровне

Любая схема, разработанная для обеспечения безопасности сети, должна быть реализована на некотором уровне протоколов, как показано на диаграмме ниже (рис. 1)

Layer	Communication Protocols	Security Protocols
Application Layer	HTTP FTP SMTP	PGP. S/MIME, HTTPS
Transport Layer	TCP /UDP	SSL, TLS, SSH
Network Layer	IP	IPsec

Рисунок 1. Схема безопасности сети (протоколы)

Популярной платформой, разработанной для обеспечения безопасности на сетевом уровне, является Internet Protocol Security (IPsec).

Особенности IPsec

IPsec не предназначен для работы только с TCP в качестве транспортного протокола. Он работает с UDP, а также с любым другим протоколом выше IP, таким как ICMP, OSPF и т. Д.

IPsec защищает весь пакет, представленный на уровне IP, включая заголовки более высокого уровня.

Так как заголовки более высокого уровня скрыты и содержат номер порта, анализ трафика становится более сложным.

IPsec работает от одного сетевого объекта к другому сетевому объекту, а не от процесса приложения к процессу приложения. Следовательно, безопасность может быть принята без необходимости внесения изменений в отдельные пользовательские компьютеры / приложения.

Широко используемый для обеспечения безопасной связи между сетевыми объектами, IPsec также может обеспечивать безопасность хост-хост.

Наиболее распространенным использованием IPsec является предоставление Виртуальной частной сети (VPN) либо между двумя местоположениями (шлюз-шлюз), либо между удаленным пользователем и сетью предприятия (хост-шлюз) [2].

Важные функции безопасности, предоставляемые IPsec, следующие:

-конфиденциальность (позволяет узлам связи шифровать сообщения).

-предотвращает подслушивание третьими лицами.

-аутентификация источника и целостность данных.

-обеспечивает гарантию того, что принятый пакет был фактически передан стороной, идентифицированной как источник в заголовке пакета.

-подтверждает, что пакет не был изменен или иным образом.

-ключевой менеджмент.

-позволяет безопасный обмен ключами.

-защита от определенных типов атак безопасности, таких как повторные атаки.

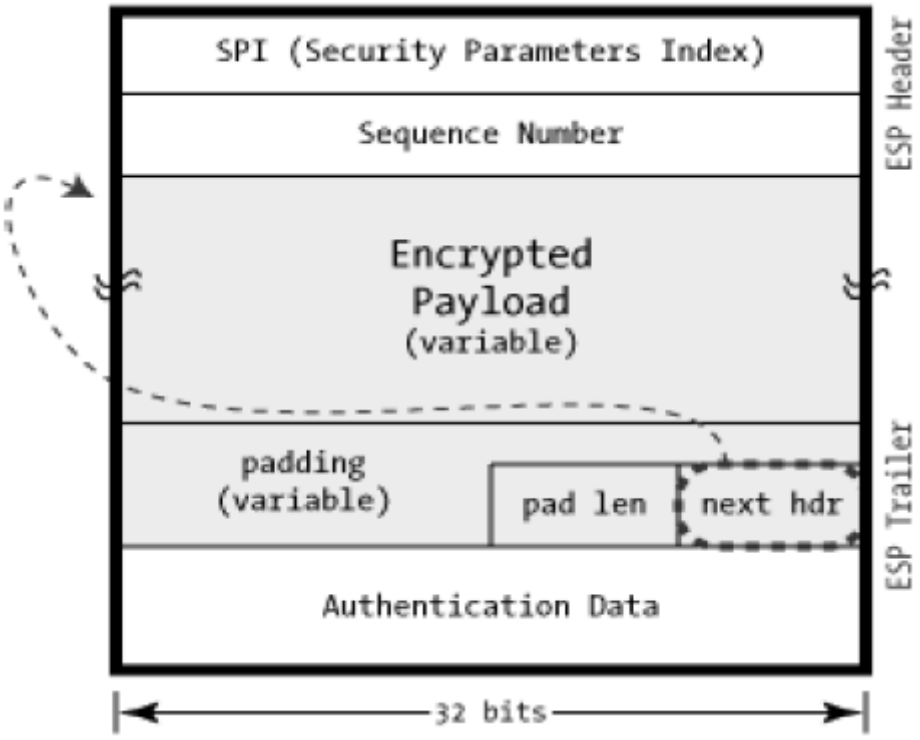
Протокол безопасности инкапсуляции (ESP)

ESP предоставляет услуги безопасности, такие как конфиденциальность, целостность, аутентификация источника и дополнительное сопротивление воспроизведению. Набор предоставляемых услуг зависит от параметров, выбранных во время создания Ассоциации безопасности (SA).

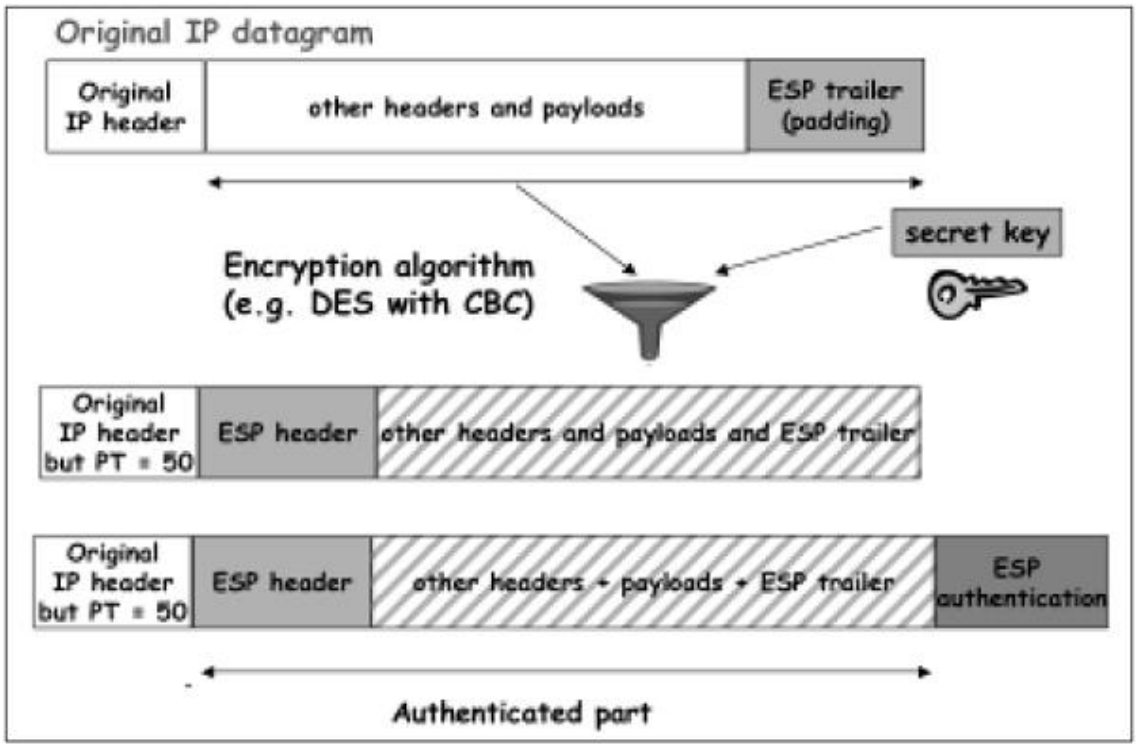
В ESP алгоритмы, используемые для шифрования и генерации аутентификатора, определяются атрибутами, используемыми для создания SA.

Процесс ESP заключается в следующем. Первые два шага аналогичны процессу , как указано выше.

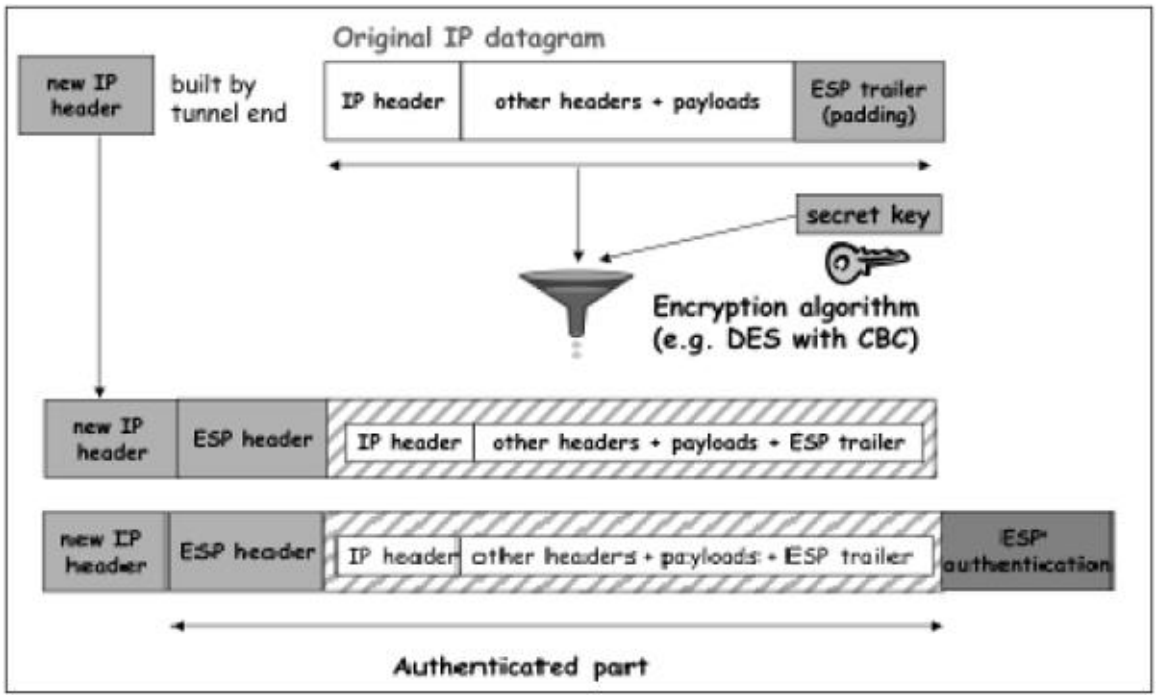
Как только определено, что ESP вовлечен, поля пакета ESP вычисляются. Расположение полей ESP изображено на следующей диаграмме.



Процесс шифрования и аутентификации в транспортном режиме изображен на следующей диаграмме.



В случае туннельного режима процесс шифрования и аутентификации такой, как изображен на следующей диаграмме.



Хотя аутентификация и конфиденциальность являются основными услугами, предоставляемыми ESP, оба являются необязательными. Технически, мы можем использовать NULL-шифрование без аутентификации. Однако на практике один из двух должен быть реализован для эффективного использования ESP.

Основная концепция заключается в использовании ESP, когда требуется аутентификация и шифрование, и использовании AH, когда требуется расширенная аутентификация без шифрования.

Ассоциации безопасности в IPsec

Ассоциация безопасности (SA) является основой связи IPsec. Особенности SA :

1.Перед отправкой данных между отправляющим объектом и принимающим объектом устанавливается виртуальное соединение, называемое «Ассоциация безопасности (SA)».

2.IPsec предоставляет множество возможностей для выполнения сетевого шифрования и аутентификации. Каждое соединение IPsec может обеспечивать шифрование, целостность, аутентичность или все три службы. Когда служба безопасности определена, два равноправных объекта IPsec должны точно определить, какие алгоритмы использовать (например, DES или 3DES для шифрования; MD5 или SHA-1 для целостности). После выбора алгоритмов оба устройства должны совместно использовать сеансовые ключи.

SA - это набор вышеуказанных параметров связи, который обеспечивает взаимосвязь между двумя или более системами для построения сеанса IPsec.

SA имеет простую природу и, следовательно, для двунаправленной связи требуются два SA.

SA идентифицируются по номеру индекса параметра безопасности (SPI), который существует в заголовке протокола безопасности.

Как отправляющий, так и принимающий объекты поддерживают информацию о состоянии SA. Это похоже на конечные точки TCP, которые также поддерживают информацию о состоянии. IPsec ориентирован на соединение, как TCP [3].

Параметры SA

Любой SA однозначно идентифицируется следующими тремя параметрами.Индекс параметров безопасности (SPI).

Это 32-битное значение, присвоенное SA. Он используется для различения различных SA, заканчивающихся в одном и том же пункте назначения и использующих один и тот же протокол IPsec.

Каждый пакет IPsec содержит заголовок, содержащий поле SPI. SPI предоставляется для сопоставления входящего пакета с SA.

SPI - это случайное число, генерируемое отправителем для идентификации SA для получателя.

IP-адрес назначения - это может быть IP-адрес конечного маршрутизатора.

Идентификатор протокола безопасности - указывает, является ли ассоциация AH или ESP SA.

Пример SA между двумя маршрутизаторами, участвующими в обмене IPsec, показан на следующей диаграмме (рис. 2)

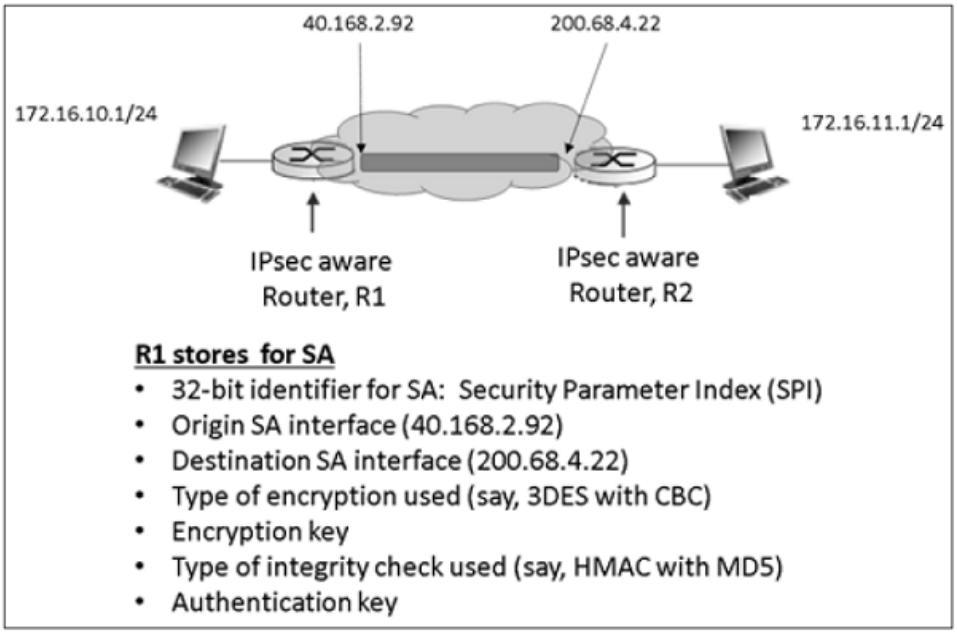


Рисунок 2. Пример SA между двумя маршрутизаторами

Безопасность административных баз данных

В IPsec есть две базы данных, которые контролируют обработку дейтаграммы IPsec. Одна - это база данных ассоциации безопасности (SAD), а другая - база данных политики безопасности (SPD). Каждая взаимодействующая конечная точка, использующая IPsec, должна иметь логически раздельные SAD и SPD

База данных политики безопасности

SPD используется для обработки исходящих пакетов. Это помогает решить, какие записи SAD следует использовать. Если запись SAD не существует, SPD используется для создания новых.

Любая запись SPD будет содержать - указатель на активный SA проводится в SAD.

Поля селектора - поле во входящем пакете с верхнего уровня, используемое для принятия решения о применении IPsec. Селекторы могут включать адрес источника и получателя, номера портов, если это уместно, идентификаторы приложений, протоколы и т. д.

Исходящие IP-дейтаграммы идут от записи SPD к конкретной SA, чтобы получить параметры кодирования. Входящая дейтаграмма IPsec попадает в правильный SA напрямую, используя тройку SPI/DEST IP/ Protocol, и оттуда извлекает соответствующую запись SAD [4].

SPD также может указывать трафик, который должен обходить IPsec. SPD можно рассматривать как фильтр пакетов, в котором решаются действия, связанные с активацией процессов SA.

Вывод

IPsec - это набор протоколов для защиты сетевых подключений. Это довольно сложный механизм, потому что вместо простого определения конкретного алгоритма шифрования и функции аутентификации, он предоставляет структуру, которая позволяет реализовать все, с чем согласны обе стороны.

Заголовок аутентификации (AH) и полезная нагрузка инкапсуляции безопасности (ESP) являются двумя основными протоколами связи, используемыми IPsec. В то время как AH только аутентифицируется, ESP может шифровать и аутентифицировать данные, передаваемые по соединению.

Транспортный режим обеспечивает безопасное соединение между двумя конечными точками без изменения заголовка IP. Туннельный режим инкапсулирует весь IP-пакет полезной нагрузки. Добавляет новый заголовок IP. Последний используется для формирования традиционного VPN, поскольку он обеспечивает виртуальный безопасный туннель через ненадежный Интернет.

Настройка соединения IPsec включает в себя все виды крипто-выбора. Аутентификация обычно строится поверх криптографического хэша, такого как MD5 или SHA-1. Алгоритмы шифрования - это DES, 3DES, Blowfish и AES. Возможны и другие алгоритмы.

Обе взаимодействующие конечные точки должны знать секретные значения, используемые при хешировании или шифровании. Ручные ключи требуют ручного ввода секретных значений на обоих концах, предположительно передаваемых каким-либо внеполосным механизмом, и IKE (Internet Key Exchange) является сложным механизмом для этого в режиме онлайн.

Список литературы:

1.Котенко И.В., Саенко И.Б., Полубелова О.В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. 1. № 25 (2). С. 113-134.

2.Беккер М.Я., Терентьев А.О., Гатчин Ю.А., Кармановский Н.С. Использование цифровых сертификатов и протоколов SSL/TLS для шифрования данных при облачных вычислениях // Научно-технический вестник информационных технологий, механики и оптики. 2016. №4

3.Alexander Endraca, Bryan King, George Nodalo, Maricone Sta. Maria, and Isaac Sabas Web Application Firewall (WAF) / Alexander Endraca, Bryan King, George Nodalo, Maricone Sta. Maria, and Isaac Sabas // International Journal of e-Education, e-Business, e-Management and e-Learning, Vol. 3, No. 6, December 2016

4.Anley, C. Advanced SQL Injection in SQL Server Applications./ Anley, C. // White Paper, Next Generation Security Software Ltd. 2015