Медведева Светлана Игоревна
магистрант
Головинский Максим Сергеевич
магистрант
ФГАОУ ВО «Национальный исследовательский университет «Московский институт электронной техники»
г. Москва

ПЕРЕДАЧА ИНФОРМАЦИИ ОБ IPSEC С ПОМОЩЬЮ ПРОТОКОЛА IKE

Аннотация: *в данной работе рассмотрен метод обмена данными о построении IPsec туннелей между сторонами. Авторами описаны различные типы пакетов и сообщений, которые используются при этом обмене. Кроме того, представлены некоторые ключевые моменты о формировании пакетов данных.*

Ключевые слова: *алгоритмы, информационная безопасность, пакеты, шифрование, IKE, IPsec.*

IKE (Internet Key Exchange – стандартный протокол IPsec) [1, с. 178] производит обмен данными о построении IPsec (набор протоколов, использующихся для обеспечения сервисов приватности и аутентификации на сетевом уровне модели OSI) туннелей между сторонами. Этот обмен может осуществляться методом комбинации main-mode и quick-mode или с помощью комбинации aggressive-mode и quick-mode. В данной работе описаны различные типы пакетов и сообщений, которые используются при этом обмене. Мы рассмотрим три типа обмена, которые могут быть в IKE:

1. Main-mode с аутентификацией на предопределённых ключах с последующим обменом в quick-mode.

2. Main mode с использованием цифровых подписей и с последующим обменом в quick-mode.

3. Aggressive mode с аутентификацией на предопределённых ключах и последующим обменом в quick-mode.

Кроме этих типов обмена, также существуют:

1. Main-mode с использованием аутентификации на нонсе с последующим обменом в quick-mode.

2. Aggressive mode с использованием цифровой подписи с последующим обменом в quick-mode.

Aggressive Mode с использованием аутентификации на предопределённых ключах. Далее речь пойдет о aggressive mode, который является альтернативой main mode. В aggressive mode используется только три сообщения, вместо шести, как в main mode. Однако скорость также имеет свою цену. Мы обозначим недостатки этого метода в конце, после того как обсудим работу aggressive mode.

IKE Фаза I (Aggressive Mode): Подготовка к отправке первого и второго сообщений. Подготовка к отправке сообщений 1 и 2 в aggressive mode представляет из себя комбинацию подготовок main mode к отправке сообщений 1, 2, 3 и 4.

Вся информация нужная для генерации секрета Диффи-Хеллмана передаётся в первых двух сообщениях, отосланных сторонами. Возможности обсудить группу Диффи-Хеллмана с помощью передачи серий предложений от инициатора к получателю – нет. Вместо этого обе стороны должны одновременно согласовать группу Диффи-Хеллмана, или обмен прервётся.

Кроме того, если метод аутентификации на предопределённых ключах используется в aggressive mode, идентификация стороны, которая также передаётся в первых двух пакетах в открытом виде. Это отличается от того же процесса в main mode обмене. Однако, преимуществом является то, что теперь с помощью ID можно найти какой стороне принадлежит предопределённый ключ. Как было отмечено в данной работе выше, main mode, ID не появится до тех пор, пока не будет найден предопределённый ключ для этого обмена.

IKE Фаза I (Aggressive Mode): Отправка первого сообщения. Первое сообщение, отправляемое инициатором, содержит в себе материал необходимый для

генерации секрета Диффи-Хеллмана получателем. Это значит, что инициатор отсылает полезную нагрузку ключа и полезную нагрузку нонса вместе со сгенерированными значениями. Также отсылается ID. Сообщение также содержит одну или несколько пар полезных предложений и преобразований для выбора получателем.

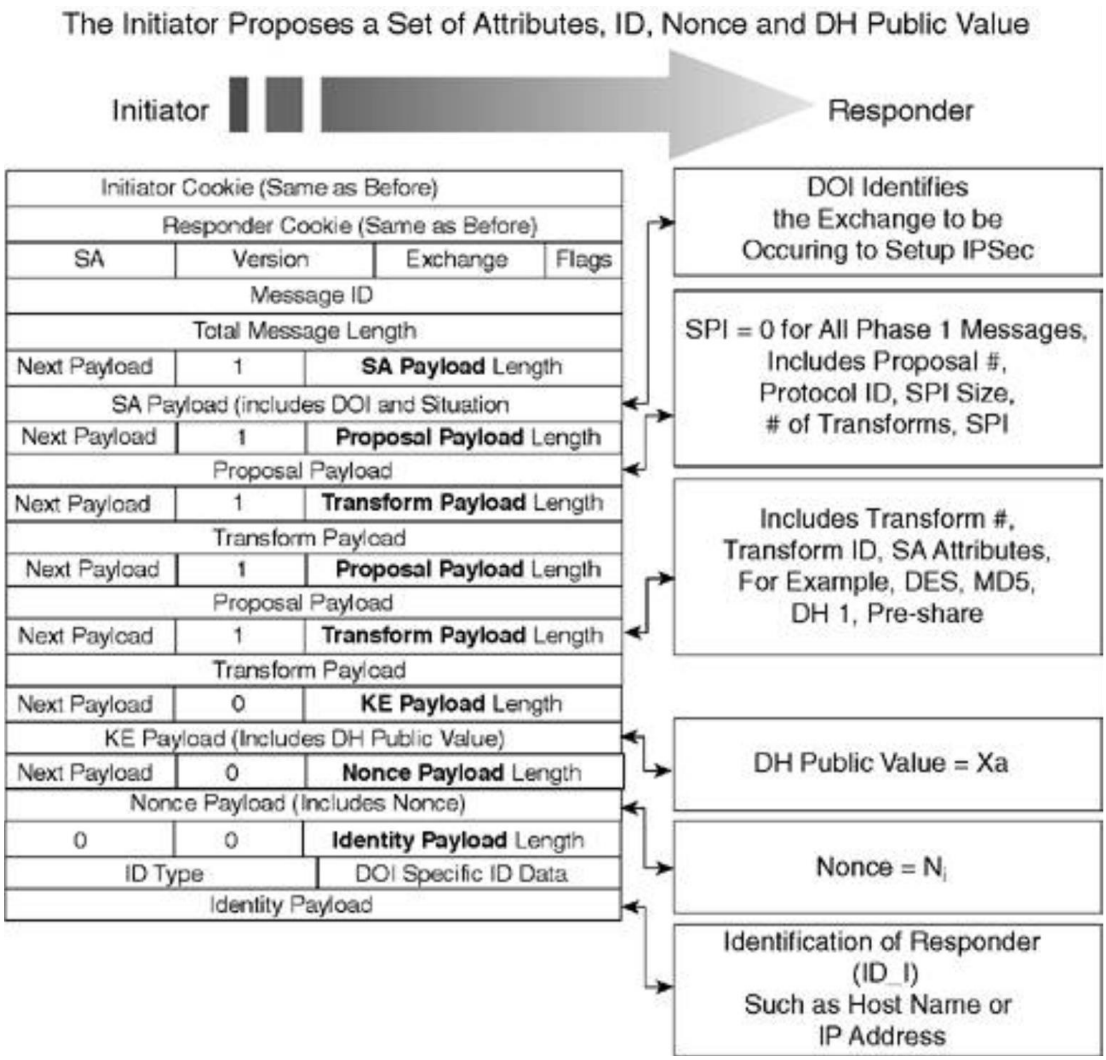

Рис. 1. Отправка первого сообщения aggressive mode от инициатора получателю

Из рисунка 1 видно, как осуществляется отправка первого сообщения aggressive mode от инициатора к получателю.

Список литературы

1. Блэк У. Интернет: протоколы безопасности [Текст] / У. Блэк. – СПб.: Питер, 2001. – 288 с.