УДК 621.391.28

Мошак Н.Н., Цветков Д.Б., Россия, Санкт-Петербург, ГУТ им. проф. М.А.Бонч-Бруевича

Оценка влияния протоколов VPN сетевого уровня на параметры транспортной системы инфокоммуникационной сети на технологии IP-QoS

Использование технологии защищенных виртуальных сетей (Virtual Private Network - VPN) позволяет обеспечить криптозащиту информации в транспорнтной системе (ТС) инфокоммуникационной сети (ИКС) общего пользования на технологии IPQoS при организации удаленного доступа пользователей к ресурсам автоматизированных систем инфоуслуг (АСИ) и/или организации защищенных каналов связи или защищенных туннелей между защищенными ЛВС корпоративных сетей.

Стандартным средством защиты межсетевого уровня IP является полнофункциональный протокол IPsec (Internet Protocol Security) [RFC 2401]. Протокол IPsec предусматривает методы аутентификации пользователей при инициации туннеля, способы шифрования конечными точками туннеля, формирования и проверки электронной цифровой подписи (ЭЦП), а также стандартные методы обмена и управления криптографическими ключами между конечными точками. ***Для функций аутентификации IPSec поддерживает цифровые сертификаты стандарта X.509.***

Архитектура средств безопасности IPSec включает в себя: протокол согласования параметров виртуального канала и управления ключами (Internet Security Association Key Management Protocol — ISAKMP), обеспечивающий общее управление защищенным виртуальным соединением, включая согласование используемых алгоритмов криптозащиты, а также генерацию и распределение ключевой информации. В отличие от протокола SKIP, протокол ISAKMP поддерживает переговоры по поводу алгоритмов шифрования и выбран в качестве обязательного протокола для управления ключами в IPSec для IPv6; ***протокол аутентифицирующего заголовка (Authentication Header — AH), предусматривающий аутентификацию источника данных, проверку их целостности и подлинности после приема, а также защиту от навязывания повторных сообщений***. В основе обеспечения целостности и аутентификации данных лежит один из приемов шифрования — шифрование с помощью односторонней функции (one-way function), называемой также ***хэш-функцией*** (hash function) или ***дайджест-функцией*** (digest function). Эта функция, примененная к шифруемым данным, дает в результате значение-дайджест, который передается в IP-пакете вместе с исходным сообщением. ***Поле Authentication Data заголовка AH — поле переменной длины,*** содержащее информацию, используемую для аутентификации пакета и называемую ***MAC-кодом (Message Authentication Code). Это поле называют также цифровой подписью, имитовставкой, хэш-значением или криптографической контрольной суммой (Integrity Check Value — ICV) пакета***. Способ вычисления этого поля определяется алгоритмом аутентификации.

Для вычисления содержимого поля Authentication Data могут применяться различные алгоритмы. В настоящее время предписывается обязательная поддержка алгоритмов HMAC-MD5 и HMAC-SHA1, основанных на применении односторонних хэш-функций (дайджест-функций) с секретными ключами. Секретные ключи генерируются в соответствии с протоколом ISAKMP.

Таким образом, независимо от режима работы, ***протокол AH*** предоставляет меры защиты от атак, ориентированных на нарушение ***целостности и подлинности*** пакетов сообщений. С помощью этого протокола аутентифицируется ***каждый пакет***, что делает программы, пытающиеся перехватить управление сеансом, неэффективными. Несмотря на нахождение IP-заголовков за пределами защищенного IPSec-конверта, протокол AH обеспечивает аутентификацию не только содержимого, но и заголовков IP-пакетов;

протокол инкапсулирующей защиты содержимого (Encapsulating Security Payload — ESP), обеспечивающий криптографическое закрытие передаваемых пакетов сообщений и предусматривающий также выполнение всех функций протокола AH. *Алгоритм применения протокола ESP к исходящим IP-пакетам* включает следующие шаги:

1. Инкапсулируемый пакет копируется в буфер.

2. Далее к этому пакету в буфере приписываются дополняющие байты (поле Padding), их число (поле Pad Length) и тип первого заголовка инкапсулируемого пакета (поле Next Header); поле Padding выбирается таким, чтобы поле Next Header было прижато к границе 32-битного слова, а размер буфера удовлетворял требованиям алгоритма шифрования.

3. Текущее содержимое буфера ***зашифровывается.***

4. В начало буфера приписываются поля SPI и Sequence Number с соответствующими значениями.

5. Пополненное содержимое буфера обрабатывается по используемому алгоритму аутентификации, и после окончания этой процедуры ***в конец буфера помещается поле Authentication Data.***

6. Формируется результирующий IP-пакет путем приписывания соответствующего IP-заголовка в начало буфера.

Протоколы AH и ESP поддерживают работу в двух режимах: туннельном и транспортном. Расположение полей заголовков протокольных блоков AH и ESP в транспортном и туннельном режимах показано на рис.1.

Транспортный режим	Туннельный режим
[IPисх.][AH][верх.]	*[IPвнеш.][AH][IPисх.][верх.]]*
[IPисх][ESP][верх.]	[Iрвнеш.][ESP][IPисх.][верх.]]
[IPисх.][AH][ESP][верх.]	

Рис.1. Расположение полей заголовков протокольных блоков в транспортном и туннельном режимах

Режимы инкапсуляции (туннелирования) и шифрования могут применяться как совместно, так и раздельно.

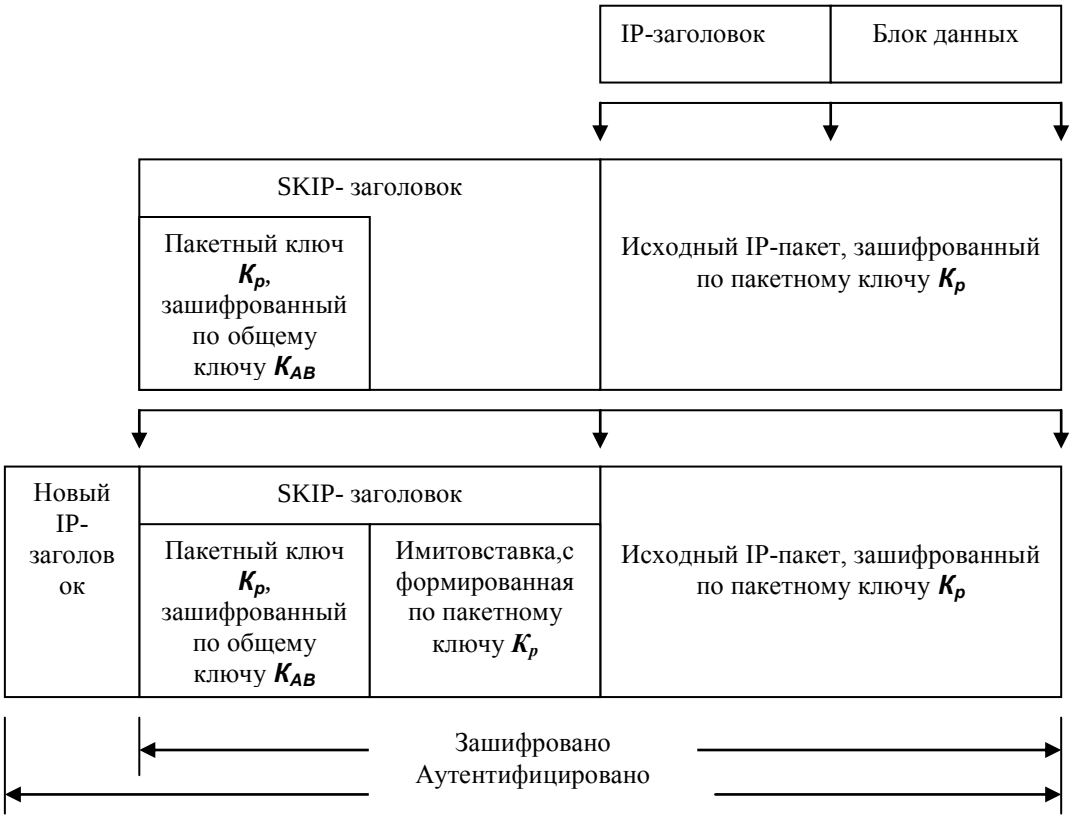

Рис. 2. IP-пакет до и после применения протокола SKIP

Для управления криптографическими ключами на сетевом уровне модели OSI наиболее широкое распространение получили такие протоколы, как SKIP (Simple Key management for Интернет Protocols) и ISAKMP. В текущей четвертой версии протокола IP (в протоколе IPv6) может применяться как протокол ISAKMP, так и протокол SKIP. ***Реализация SKIP, устанавливаемая непосредственно над IP-драйвером,*** обрабатывает весь трафик, не накладывая никаких ограничений ни на вышележащее программное обеспечение, ни на физические каналы, используемые для передачи информации. Технология распределения ключей основана на асимметричной криптосистеме Диффи-Хеллмана. ***Процедура формирования зашифрованного пакета*** с применением протокола SKIP приведена на рис. 2.

1. Исходный IP-пакет ***зашифровывается*** по пакетному ключу Кр и инкапсулируется в SKIP-пакет.

2. Пакетный ключ K_p зашифровывается по общему секретному ключу K_{AB} и помещается в SKIP-заголовок; при этом в SKIP-заголовке резервируется поле под эталонную характеристику результирующего IP-пакета.

3. Полученный SKIP-пакет инкапсулируется в результирующий IP-пакет.

4. Для результирующего IP-пакета с помощью хэш-функции рассчитывается по пакетному ключу K_p эталонная характеристика и полученное значение помещается как имитовставка в зарезервированное поле SKIP-заголовка.

Приведем *алгоритм работы протокола Ipsec*:

1. по адресу IP получателя выбрать алгоритм шифрования, ЭЦП и криптографические ключи. Если адрес получателя имеется в настройках, то перейти к п.2;

2. сгенерировать ЭЦП или вычислить ИВ и добавить в пакет;

3. зашифровать пакет;

4. сформировать заголовок VPN-агента и инкапсулировать зашифрованный пакет;

5. отправить пакет VPN-агенту;

6. при получении пакета аутентифицировать отправителя по его адресу. Если адрес имеется в списке разрешенных и пакет не поврежден, то перейти к п.7;

7. выбрать алгоритм шифрования, ЭЦП и криптографические ключи;

8. расшифровать пакет и проверить целостность. Если целостность не нарушена, то перейти к п.9;

9. отправить исходный пакет в защищенный сегмент корпоративной ЛВС получателю.