УДК 681.3.06: 519.248.681

А. В. СВИНАРЕВ канд. тех. наук, А. Н. ЛЕПЕХА, Р. В. ОЛЕЙНИКОВ,
А. И. ШУМОВ, А. А. ГАЙОВИЧ, А. А. КАЗЬМИН

ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПРОТОКОЛА IPSec

Введение

Бурное развитие сети Internet привело к проникновению новых информационных технологий практически во все сферы человеческой деятельности. Благодаря этому процессу стал возможным и обыденным ежедневный обмен сообщениями для пользователей с разных континентов, для работы и развлечения доступны гигантские массивы информации, множество организаций и ведут единый электронный документооборот в территориально разнесённых филиалах, множество фирм получили возможность вести бизнес из любой точки мира, где есть доступ к Сети. Дистанционное образование, дешевые международные телефонные переговоры, возможность найти интересующую информацию практически по любому вопросу, консультации множества специалистов были бы невозможны без происходящей информационной революции.

1. Основные угрозы, возникающие в IP-сетях

Своим рождением сеть Internet во многом обязана протоколу IP, на основании которого построены большинство национальных, корпоративных и академических сетей. Такая популярность вызвана его гибкостью, надёжностью и удобством в обслуживании. Неоспоримыми преимуществами IP является гибкость и простота маршрутизации пакетов, передаваемых по сети. Благодаря поддержке на подавляющем большинстве современных платформ, он является идеальным средствам построения негетерогенных сетей и является неотъемлемой частью широко распространённых операционных систем, таких как Unix и Windows.

Поскольку протокол IP появился более 30 лет назад, его разработчики не могли предвидеть столь широкое распространение, а также проблемы, возникающие в связи с этим. Сети, базирующиеся на протоколе IPv4 (наиболее распространённые в настоящее время), не имеют встроенных средств обеспечения безопасности взаимодействующих узлов, что связано со структурой самого протокола. Вместе со всеми преимуществами, гибкость IP протокола позволяет реализовать ряд опасных угроз:

- Spoofing – подмена IP-адресов, в результате чего невозможно гарантировать подлинность взаимодействующих сторон;
- Sniffing – приём всех IP-пакетов, пересылаемых по определённому сегменту сети, что даёт злоумышленнику возможность получить всю переданную по сети информацию;
- Highjacking – это комбинация первых двух методов, когда после установления соединения злоумышленник отключает легального абонента и вступает в информационный обмен вместо него.

Существуют различные решения проблемы обеспечения безопасности взаимодействующих сторон. Одним из вариантов является использованием современных криптографических алгоритмов на прикладном уровне (в соответствии с семиуровневой моделью OSI). Наиболее яркий пример – использование пакета PGP для обеспечения целостности, подлинности, аутентичности и конфиденциальности файлов, передаваемых по сети. Другим вариантом может стать применение семейства протоколов SSL/TLS для защиты на транспортном уровне.

Недостатком первого решения является невозможность обеспечить прозрачное для пользователя взаимодействие в реальном масштабе времени. Второе решение требует наличия специальных сетевых приложений с поддержкой SSL/TLS и кроме того, использование защиты на транспортном уровне (и выше) не позволяет скрыть топологию взаимодействия, что даже при использовании криптографических методов позволяет злоумышленнику получать информацию о взаимодействующих узлах, а также проводить атаки типа DoS (Denial of Service – отказ в обслуживании). Защита на прикладном уровне эффективна для электронной почты, на транспортном – для ведения электронной коммерции, однако для других задач, например при построении защищенных корпоративных сетей, этого явно недостаточно.

Наиболее универсальным и эффективным решением является обеспечение защиты на сетевом уровне. Поскольку на разных уровнях взаимодействуют различные протоколы, в зависимости от архитектуры сети и типа коммуникации, но, в конце концов, вся информация, подлежащая передаче по сети, поступает на сетевой уровень, где для информационного обмена используется только один протокол – IP. Таким образом, обеспечение безопасности сетевого уровня обеспечивает защиту любых соединений в сети для всех приложений. Более того, эти услуги совершенно прозрачны для пользователя и приложений.

2. Архитектура стандарта IPSec

Для защиты сетевого протокола следующей версии (IPv6) был разработан IP Security Protocol (IPSec). Его основные функции – обеспечение конфиденциальности и целостности передаваемых пакетов, сокрытие топологии взаимодействия в сети, аутентификации источника сообщений, а также защита против атак типа replay (повторного приёма пакетов) и DoS. Однако благодаря гибкости и масштабируемости IPSec совместим и с используемым IPv4.

К настоящему моменту на Украине нет литературы, которая бы описывала и проводила анализ IPSec протокола. Цель данной статьи восполнить этот пробел и описать принципы работы IPSec и способы, с помощью которых он предоставляет безопасность функционирования IP протокола. Другой задачей будет предоставить описание управления ключевыми структурами в открытых сетях между взаимодействующими сторонами.

IPSec предоставляет все необходимые средства для построения виртуальных защищённых сетей (VPN — Virtual Private Network) на основании открытых каналов связи. С помощью IPSec можно обеспечить защищенные каналы между произвольными сетями, используя для этого любые незащищенные линии коммуникации, например, Internet.

Существует два вида реализации протокола IPSec, предлагаемых в [1]:

- Программное решение, в виде драйвера для операционной системы – Bump-in-the-Stack (BITS);
- Аппаратное решение, с встроенной специализированной операционной системой – Bump-in-the-Wire (BITW).

BITS добавляет дополнительный заголовок в стек протокола TCP/IP (рис.1).

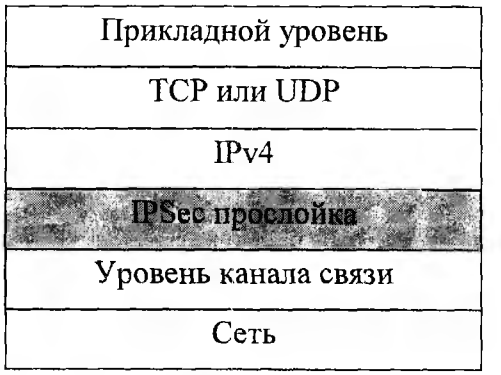

Рис. 1

Аппаратная реализация (BITW), представляет собой некоторое криптографическое устройство со специализированной операционной системой (шлюз), находящееся между защищенной локальной сетью и любой открытой сетью, через которую происходит взаимодействие с другой защищённой сетью.

IPSec функционирует в двух режимах:

- Транспортном;
- Туннельном.

В транспортном режиме IPSec обеспечивает защиту для транспортного уровня и выше (для TCP/UDP протоколов). В этом случае используется схема встраивания заголовка IPSec между заголовком IP и TCP (рис. 2). Заголовок IP не модифицируется и передается в открытом виде, защищенном только кодом аутентификации (HMAC).

Недостаток этого режима в том, что он не обеспечивает сокрытия топологии сети. К преимуществам можно отнести то, что этот режим полностью прозрачен для приложений, в отличие от TLS/SSL протоколов.

IP заголовок	IPSec заголовок	TCP/UDP заголовок	Данные

Рис. 2

Туннельный режим обеспечивает конфиденциальность всего пакета, включая и IP заголовок, как показано на рис.3.

Новый IP заголовок	IPSec заголовок	IP заголовок	TCP/UDP заголовок	Данные

Рис. 3

Этот режим также позволяет разрешить проблему использования зарезервированных адресов, которые недопустимо использовать в Internet. Как правило, при реализации этого варианта между открытой сетью и защищенной локальной сетью ставиться специальное устройство – шлюз, которое выполняет все необходимые функции.

Существует две реализации туннельного режима:

- Сеть-в-сеть (network-to-network);

- Узел-в-сеть (host-to-network).

В первом случае (сеть-в-сеть) используется связь между двумя виртуальными частными сетями, имеющих свои внутренние адреса, через специализированные устройства.

Во втором случае происходит связь между закрытой виртуальной сетью со шлюзом и некоторым узлом, с допустимым для Internet адресом, в открытой сети.

Стандарт IPSec – набор протоколов и компонентов. Базовый комплект состоит из следующих протоколов:

1. ISAKMP – Internet Security Association and Key Management Protocol – определяет правила инициализации SA (Security Association) – защищенного соединения. Задаются методы начальной аутентификации сторон, выбора метода установки защищенного канала и выработка общего секрета. Базируется на алгоритме Диффи-Хеллмана.
2. IKE – Internet Key Exchange – Задает правила установки безопасного соединения. Могут создаваться несколько защищенных соединений для разных категорий трафика. Использует общий секрет, полученный с помощью ISAKMP для генерации ключей. Кроме IP, может использоваться и с другими протоколами.
3. AH – Authentification Header – Обеспечивает целостность, аутентификацию и защиту от повторения пакетов. Это протокол, имеющий стандартный номер 51;
4. ESP – Encapsulating Security Payload – Обеспечивает конфиденциальность, целостность, аутентификацию и защиту от повторения. Протокол имеет стандартный номер 50.

Рассмотрим каждый из протоколов более подробно.

3. Управление ключами в IPSec

ISAKMP – это первая фаза работы IPSec протокола. По умолчанию протокол ISAKMP использует IKE протокол, который функционирует в 3-х режимах, используя первые два режима протокола IKE (Основной или Активный) для установления безопасного канала соединения [2].

Активный и Основной режимы практически одинаковы за исключением того, что А4ктивный режим использует меньшее число обменов, но не предоставляет аутентификационную защиту взаимодействующих узлов, так как стороны передают свои идентификаторы до того, как будет установлен безопасный канал. Оба режима еще будут рассмотрены далее в статье.

По сути, протокол ISAKMP должен установить безопасный канал для будущих обменов ключами. В результате его работы в одном из приведенных выше режимов, стороны должны выбрать поддерживаемый обеими сторонами алгоритм шифрования, хеширования, псевдослучайную функцию, метод аутентификации, выработать общий секрет и тип защиты – ESP, AH, либо оба совместно.

Основной режим выполняется в три этапа с использованием двухсторонних обменов (рис. 4). Сначала стороны обмениваются базовыми алгоритмами и хешами (пункт 1 и 2 на рис. 4). Далее (пункт 3 и 4) они обмениваются открытыми ключами по Диффи-Хеллману и обмениваются случайными числами, которые другая сторона обязана подписать и вернуть для своей идентификации. И, наконец, (пункт 5 и 6) они проверяют полученные идентификаторы.

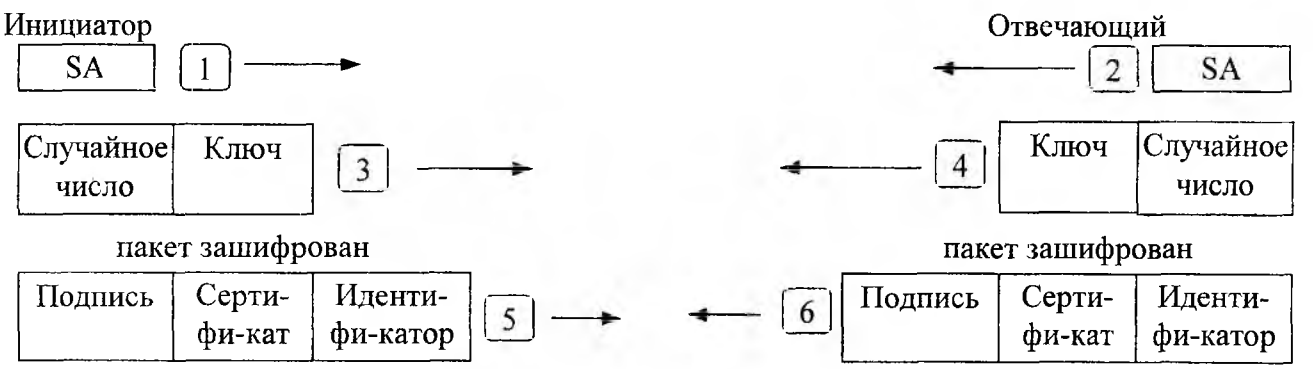

Рис. 4

Активный режим (рис. 5), являющийся упрощенной альтернативой Основному режиму, выполняется за три этапа, но в данном случае нарушается идентификационная защита, что открывает путь для атаки типа man-in-the-middle. Таким образом, эта схема будет непригодна для соединений, требующих надёжной защиты.

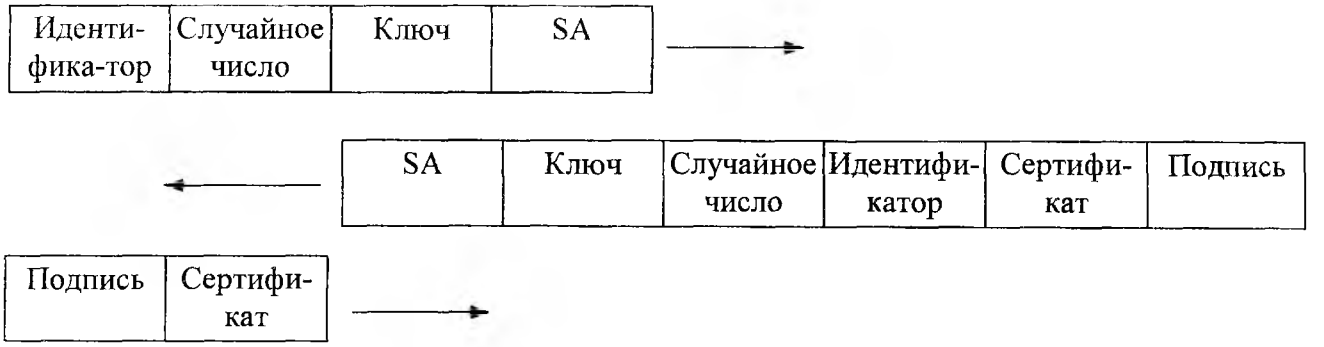

Рис. 5

При двухстороннем обмене стороны обмениваются псевдослучайными числами. Данное число можно получить как результат работы хеш-алгоритма. Для повышения безопасности лучшим вариантом будет использование криптографических генераторов случайных чисел. Существуют и другие *варианты работы ISAKMP протокола, описываемые в источнике [3].* Схема их работы похожа на приведенные выше схемы (рис. 4, 5). И более того, в них имеется много недостатков, которые будут рассмотрены ниже.

Перейдем к рассмотрению работы IKE протокола в Быстром режиме. Его задача, используя установленный предыдущими обменами защищенный канал, задать список общих IPSec сервисов и обновить или сгенерировать ключи.

Работа этого режима выглядит аналогично Активному режиму (рис. 5) при работе ISAKMP (IKE) протокола в Основном режиме. Однако при работе протокола IKE в Быстром режиме все пакеты шифруются и всегда передаются с хеш-значением, поэтому здесь гарантируется конфиденциальность и целостность передаваемых данных. Общие ключи могут получаться либо хешированием уже существующих ключей, полученных при работе ISAKMP протокола, либо стороны обмениваются случайными числами через установленный безопасный канал и используют хеш этих чисел как сеансовый ключ для работы.

При работе этого протокола вырабатывается также общий набор поддерживаемых алгоритмов шифрования, аутентификации, хеширования и генерации ключей. Весь этот набор заноситься в базу данных. Далее стороны вырабатывают так называемый SPI (Security Parameter Index) – число, с помощью которого обе стороны смогут в последствии делать предложения по использованию желательного набора правил для данного соединения. SPI вырабатывается совместно с IP адресом, протокольными данными и тем самым уникально идентифицирует этот набор IPSec SA, который должен быть идентичен для обеих сторон.

Возможно, лучшим решением было бы создание этих IPSec SA для каждого нового соединения, что будет включать и генерацию новых ключей. Это позволит производить частую смену ключей и воспрепятствует статистическому накоплению данных атакующим.

4. Криптографические преобразования в IPSec

Следующим компонентом, входящего в состав IPSec, является протокол AH, описываемый в документе [4]. Его цель состоит в предоставлении услуг аутентификации для IP пакета, но он не решает проблему конфиденциальности. Этот протокол используется либо сам по себе, либо совместно с протоколом ESP, который будет рассмотрен ниже.

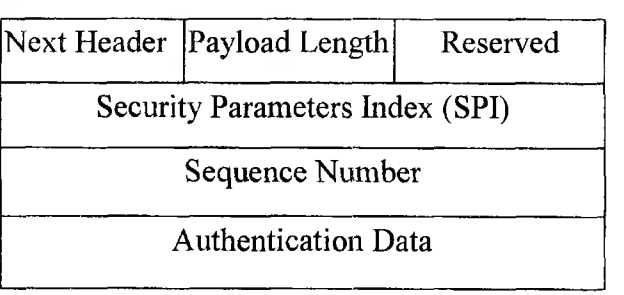

Рис. 6

На рис. 6 представлен заголовок протокола AH. Опишем его поля:

- Next Header – задает следующий (вложенный) протокол (либо TCP, либо UDP);
- Payload length – длина заголовка AH (может изменяться в зависимости от используемых алгоритмов аутентификации;
- Sequence Number – номер пакета. Служит для предотвращения повтора пакетов;

- SPI – служит для сопоставления пакета конкретному SA (защищенному каналу);
- Authentication Data – содержит ICV (Integrity Check Value), который формируется на основе кодов аутентификации заголовка IP пакета и его данных, используя 16-байтный хеш. Обязательной является поддержка алгоритмов HMAC-MD5-96 и HMAC-SHA-96.

АН протокол можно использовать как в транспортном режиме, чтобы защитить протоколы и данные верхнего уровня, так и в туннельном режиме, защищая весь пакет в целом. На рис. 7 показано встраивание заголовка АН в IP пакет.

IPv4 заголовок PROTOCOL=51	АН заголовок NEXT HEADER=6	TCP/UDP заголовок	Данные

Рис. 7

В транспортном режиме некоторые из полей IP заголовка не могут быть включены в процесс получения ICV из-за того, что они могут изменяться во время передачи. Поэтому вариантом усиления защиты может быть использование туннельного режима работы.

Оставшийся протокол, который необходимо рассмотреть – ESP, обеспечивает конфиденциальность передаваемых данных с помощью шифрования [5]. Подобно АН протоколу он также предоставляет услуги целостности, аутентификации и обнаруживает повторно принятые пакеты. Однако, в отличие от протокола АН, аутентифицируется не весь пакет, а только инкапсулированные в него данные, как показано на рис. 8.

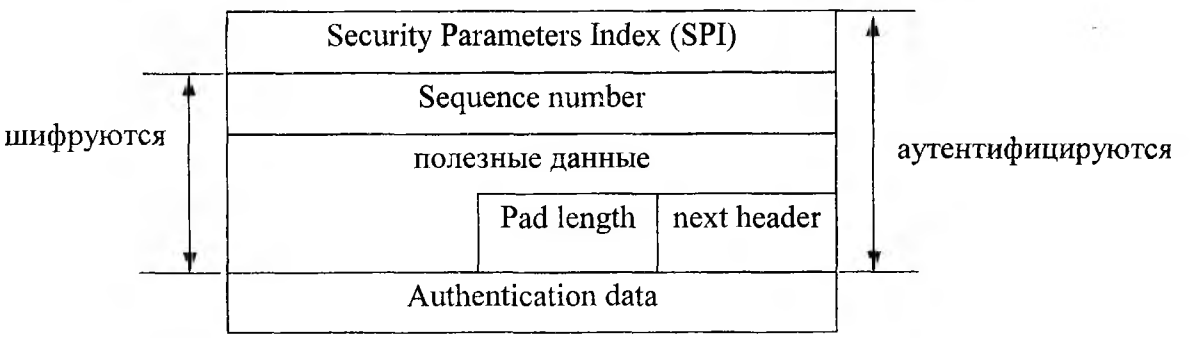

Рис. 8

Опишем представленные в ESP протоколе поля:

- SPI – служит для сопоставления пакета конкретному SA (защищенному каналу);
- Sequence Number – номер пакета, служит для предотвращения повторного приёма пакетов;
- Initialization Vector – 64-битовый случайный вектор, используемый для шифрования (необходим для режима CBC алгоритма DES, используемого для шифрования данных);
- Protected Data – зашифрованное содержимое IP пакета (в транспортном режиме), либо весь пакет целиком (в туннельном режиме). Для шифрования используется алгоритм шифрования DES (длина ключа 56 бит), а также возможно использование TDES (длина ключа 168 бит) и IDEA (128 бит);
- Pad Length – длина дополнения данных для выравнивания по 8-байтовой границе (требование режима CBC алгоритма шифрования DES);
- Authentication Data – данные аутентификации.

Протокол ESP встраивается в IP пакет сразу после заголовка, как показано на рис. 9. Он может использоваться как сам по себе, так и совместно с протоколом АН.

IPv4 заголовок PROTOCOL=50	ESP заголовок NEXT HEADER=6	АН заголовок NEXT HEADER=6	TCP/UDP заголовок	данные

Рис. 9

5. Недостатки IPSec

Анализируя набор IPSec протоколов, можно сказать, что в целом выбор IPSec будет одним из лучших вариантов решения при создании VPN, как с точки зрения безопасности, так и с точки зрения удобства для пользователей и экономической выгоды. Это позволяет использовать открытые сети без привлечения специализированных линии связи.

Однако IPSec имеет некоторые недостатки, которые должны учитываться при разработке протокола.

Как отмечается в [6], стандарт IPSec является слишком сложным, чтобы провести полный анализ его безопасности, что делает весьма вероятным выявление в будущем каналов уязвимости. Другими следствиями высокой сложности стандарта являются:

1. В документации по IPSec не определяются задачи защиты, функциональность не продумана: некоторые протоколы являются функционально избыточными (например, AH), и вместе с тем некоторые протоколы неполно обеспечивают некоторые услуги, (обмен сертификатами).
2. Администраторы безопасности могут допускать ошибки при конфигурировании системы защиты. Например, ассоциации безопасности в IPSec являются однонаправленными, следовательно, систему можно сконфигурировать так, чтобы защита выполнялась для исходящего трафика и не выполнялась для входящего.
3. Документация трудна для чтения и содержит ошибки.

Кроме этого, в [6] приведены и другие замечания по стандарту.

Во-первых, AH протокол защищает не все поля IP заголовка, поэтому при использовании в критичных, с точки зрения безопасности, системах, особенно в банковских, следует использовать туннельный режим работы. Лучше всего для этого использовать специализированное аппаратное криптографическое устройство. При этом можно исключить протокол AH из работы, а протокол ESP должен всегда включать аутентификацию.

Другим недостатком можно считать предлагаемые к использованию криптографические алгоритмы. В частности, в протоколе ESP базовым является DES (ключ длиной 56 бит). Сегодня он уже не обеспечивает требуемый уровень безопасности. В будущих вариантах протокола IPSec предлагается его надо исключить даже для применения в не требующих особой защиты системах. Альтернативные алгоритмы TDES и IDEA также со временем потребуют замены. К настоящему времени как стандарт XXI века принят криптографический симметричный алгоритм RIJNDAEL, главным достоинством которого является отсутствие каких-либо эффективных криптоаналитических атак, кроме прямого перебора. Для аутентификации можно применять современные алгоритмы на эллиптических кривых, обладающих высокой стойкостью. Следует заметить и о возможной замене обычного алгоритма Диффи-Хеллмана стандартом X.9-63 – Диффи-Хеллман на эллиптических кривых для использования в протоколах ISAKMP и IKE. Несомненным достоинством IPSec протокола является возможность подключения новых криптографических алгоритмов. Таким образом, устранить перечисленные недостатки не составляет особого труда.

Стоит отметить ошибку, которая скрыта в функционировании протокола ESP. Как уже отмечалось ранее, данный протокол сначала осуществляет зашифрование и лишь потом аутентификацию. Такой режим работы открывает дорогу ряду атак. Решением здесь может стать либо изменение порядка операций – сначала аутентификация, потом зашифрование – либо подписывать ключ шифрования вместе с зашифрованным текстом.

В документации по протоколу IPSec, как уже отмечалось ранее, рекомендуется использовать криптографические алгоритмы шифрования в режиме CBC. Однако в данном режиме высока вероятность коллизий, а также усложняется аппаратная реализация протокола. Этот факт следует учитывать в будущих разработках.

Помимо перечисленных выше недостатков спецификация протокола допускает использование переменного числа циклов в шифре, что ослабляет криптографическую стойкость. Следует убрать эту возможность.

Как уже упоминалось, протокол ISAKMP имеет различные схемы реализации и является в действительности набором протоколов, которые обязаны установить безопасный канал. В статье было рассмотрено использование протокола ISAKMP как работа первых двух режимов протокола IKE. Предоставленные в источнике [1] схемы обменов имеют существенные недостатки. Так в некоторых типах обменов, предоставляемых этим протоколом, имеется вероятность осуществления известных атак. Базовый режим в [1] аналогичен Активному режиму в Основном режиме работы протокола IKE. Недостатком здесь является отсутствие идентификационной защиты, что открывает путь для

атаки man-in-the-middle. Аналогичная атака возможна при использовании режима Аутентификация (Authentication Only Exchange), где вообще не осуществляется шифрование. Анализ показал, что предлагаемые схемы не предоставляют полной защиты как от replay (повтор пакета), так и DoS (отказ в обслуживании) атак. Это вызвано плохой продуманностью предлагаемой архитектуры протокола ISAKMP, о чем говорят ошибки, встречающиеся в документации и слишком общее описание его работы.

В рассматриваемом варианте, с использованием протокола IKE, имеется возможность осуществления атаки типа proposal, которая подразумевает под собой, что злоумышленник может навязать использование сторонами ослабленных вариантов криптографических алгоритмов (с малой длиной ключа, либо использование устаревших алгоритмов и т.п.). Это можно увидеть, анализируя Основной режим, представленный на рис. 4.

Еще одно замечание относительно протокола IKE, которое рассматривалось на конференции посвященной протоколу IPSec и проходившей во Франции в октябре 2000 года, заключалось в том, что протокол IKE при работе идентифицирует только удаленный компьютер, но не самого пользователя. Таким образом, при его работе используются сертификаты компьютера, но не самого пользователя. Как показывает практика, наибольшее количество нарушений безопасности вызывается самими служащими, а не внешними злоумышленниками. Поэтому данный момент требует обратить на себя внимание. На данный момент некоторые зарубежные корпорации предлагают использование дополнительных протоколов, которые позволяют осуществлять аутентификацию пользователя. Так, например, фирма Microsoft в собственных разработках протокола IPSec применяет протокол L2TP, который функционирует совместно с IPSec, работающим в туннельном режиме.

Тем не менее, несмотря на приведенные замечания, IPSec является на сегодняшний день лучшим стандартом защиты на сетевом уровне.

Заключение

На основании вышеизложенного материала можно говорить о том, что в целом, учитывая замечания, указанные в статье, применение протокола IPSec будет наиболее универсальным средством для решения задач обеспечения безопасности при взаимодействии в открытых сетях. Данная тема является одной из самых популярных за рубежом. Об свидетельствуют многочисленные публикации в журналах и Интернете, ежегодные конференции посвященные протоколу IPSec, на которых обсуждаются пути улучшения его функциональности. Многие компании предлагают свои услуги по тестированию продуктов реализующих протокол IPSec, предъявляя конкретные требования к конкурсантам. Многие из этих требований уже фактически стали стандартами для этого протокола. Предпосылками для внедрения IPSec протокола на отечественном рынке может служить то, что сегодня на рынке господствуют операционные системы зарубежных стран, которые не отвечают требованиям необходимой степени защиты и не дают гарантии, что в них не имеется закладок, оставленных разработчиками. Использование таких операционных систем в требующих повышенной безопасности организациях слишком большой риск. Не меньший риск и покупка средств защиты, предлагаемых на иностранных рынках. Поэтому внедрение IPSec, разработанного отечественными специалистами, позволит решить эти проблемы наиболее универсальным способом.

Список литературы: 1. *Ken Masica.* Understanding the IP Security Protocol // Internet Security. Oct. 2000. Vol.3. No. 5. pp. 38-42. 2. *RFC 2409.* The Internet Key Exchange (IKE), Request for Comments: 2409 / Network Working Group, 1998. 3. *RFC 2408.* Internet Security Association and Key Management Protocol (ISAKMP), Request for Comment 2408. / Network Working Group, 1998. 4. *RFC 2402.* IP Authentication Header (AH), Request for Comments: 2402 / Network Working Group, 1998. 5. *RFC 2406.* IP Encapsulating Security Payload (ESP), Request for Comments: 2406 / Network Working Group, 1998. 6. *Niels Ferguson, Bruce Schneier.* A Cryptographic Evaluation of IPsec. /Counterpane Internet Security, Inc., 1999.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 29.03.2001