может быть проведен для каждого из полученных эффективных уравнений после того, как будут указаны биты (согласно данному уравнению), участвующие в анализе, а также вероятность, с которой данное уравнение выполняется. Результатом анализа будет являться заполнение таблицы результата, состоящей из четырех полей. Первое поле (обозначенное буквой N) отображает количество текстов, участвующих в анализе; второе поле (обозначенное буквой P) по сути дела отображает введенную студентом вероятность; третье поле (обозначенное буквой T) показывает число открытых текстов, для которых левая часть эффективного уравнения равна 0; и последнее четвертое поле содержит результат анализа, а именно то значение, которому соответствует правая часть данного эффективного уравнения.

Правильность анализа может быть проверена введением всех найденных битов в «Форму» проверки. Те биты, которые определить невозможно должны быть помечены как x. Если все биты, которые было возможно определить найдены верно, то программа выдаст соответствующее сообщение Для выполнения лабораторной работы по изучению дифференциального криптоанализа разработанна программа Krypto1.exe. С помощью данной программы для каждого варианта производится зашифрование указанного числа открытых текстов на определенном ключе. Также для каждого из этих открытых текстов подбирается парный текст, согласно указанному значению ΔA, который в свою очередь зашифровывается на том же ключе. Если получившиеся пары выходов удовлетворяют указанному значению ΔC, то данные пары текстов выводятся на экран. После этого студент имеет возможность сохранить либо напечатать полученные результаты для удобства дальнейшей работы. Проверка правильности найденных битов ключа осуществляется аналогично описанной выше проверки для работы по изучению линейного криптоанализа.

Библиографический список

1. *А. Чмора,* Современная прикладная криптография, М.: «Гелиос АРВ», 2002.
2. *Б. Шнайер,* Прикладная криптография, М.: «Издательство ТРИУМФ», 2002.
3. *А.А. Грушо, Е.Е. Тимонина, Э.А. Применко,* Анализ и синтез криптоалгоритмов. Курс лекций. Йошкар-Ола, издательство МФ МОСУ, 2000.

Ю.Н. Бельтриков, А.Ю. Коробко
Россия, г. Таганрог, ТРТУ, г. Нальчик, НИИ ПМА КБНЦ РАН

ПРОТОКОЛ IPSEC: ИСПОЛЬЗОВАНИЕ РОССИЙСКИХ СТАНДАРТОВ ШИФРОВАНИЯ

Введение

Базовые механизмы информационного обмена в сетях TCP/IP были в целом сформированы в начале восьмидесятых годов и направлены на обеспечение доставки пакетов данных между различными операционными системами с использованием разнородных каналов связи. Несмотря на то, что идея создания сети ARPANet принадлежала правительственной оборонной организации, фактически сеть зародилась в исследовательском мире и наследовала традиции открытости академического сообщества. Ещё до коммерциализации Интернета (которая произошла в середине девяностых годов) многие авторитетные исследователи отмечали проблемы, связанные с безопасностью стека протоколов TCP/IP. Основные концепции протоколов TCP/IP не полностью удовлетворяют (а в ряде случаев и противоречат) современным представлениям о компьютерной безопасности.

До недавнего времени сеть Интернет использовалась в основном для передачи информации по относительно простым протоколам: электронная почта, передача файлов, удалённый доступ. Сегодня, благодаря широкому распространению

технологий WWW, всё активнее применяются средства распределённой обработки мультимедийной информации. Одновременно с этим растёт объём данных, обрабатываемых в средах клиент/сервер и предназначенных для одновременного коллективного доступа большого числа абонентов. Разработано несколько протоколов прикладного уровня, обеспечивающих информационную безопасность таких приложений, как электронная почта (PEM, PGP и т.п.), WWW (Secure HTTP, SSL и т.п.), сетевое управление (SNMPv2 и т.п.). Однако наличие средств обеспечения безопасности в базовых протоколах семейства TCP/IP позволяет осуществлять информационный обмен между широким спектром различных приложений и сервисных служб.

В 1994 году Совет по архитектуре Интернет (IAB) выпустил отчет "Безопасность архитектуры Интернет". В этом документе описывались основные области применения дополнительных средств безопасности в сети Интернет, а именно, защита от несанкционированного мониторинга, подмены пакетов и управления потоками данных. В числе первоочередных и наиболее важных защитных мер указывалась необходимость разработки концепции и основных механизмов обеспечения целостности и конфиденциальности потоков данных. Поскольку изменение базовых протоколов семейства TCP/IP вызвало бы полную перестройку сети Интернет, была поставлена задача обеспечения безопасности информационного обмена в открытых телекоммуникационных сетях на базе существующих протоколов. Таким образом, начала создаваться спецификация Secure IP, дополнительная по отношению к протоколам IPv4 и IPv6.

Архитектура IPSec

IP Security - это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов; в его состав сейчас входят почти 20 предложений по стандартам и 18 RFC (Рис.1).

Спецификация IP Security (известная сегодня как IPsec) разрабатывается Рабочей группой IP Security Protocol IETF. Первоначально IPsec включал в себя 3 алгоритмо-независимые базовые спецификации, опубликованные в качестве RFC-документов "Архитектура безопасности IP", "Аутентифицирующий заголовок (AH)", "Инкапсуляция зашифрованных данных (ESP)" (RFC1825, 1826 и 1827). Необходимо заметить, что в ноябре 1998 года Рабочая группа IP Security Protocol предложила новые версии этих спецификаций, имеющие в настоящее время статус предварительных стандартов, это RFC2401 - RFC2412. Отметим, что RFC1825-27 на протяжении уже нескольких лет считаются устаревшими и реально не используются. Кроме этого, существуют несколько алгоритмо-зависимых спецификаций, использующих протоколы MD5, SHA, DES.

Заголовок AH

Заголовок аутентификации (AH) является опциональным заголовком и, как правило, располагается между основным заголовком пакета IP и полем данных. Наличие AH никак не влияет на процесс передачи информации транспортного и более высокого уровней. Основным и единственным назначением AH является обеспечение защиты от атак, связанных с несанкционированным изменением содержимого пакета, и в том числе от подмены исходного адреса сетевого уровня. Протоколы более высокого уровня должны быть модифицированы в целях осуществления проверки аутентичности полученных данных.

Заголовок ESP

В случае использования инкапсуляции зашифрованных данных заголовок ESP является последним в ряду опциональных заголовков, "видимых" в пакете. Поскольку основной целью ESP является обеспечение конфиденциальности данных, разные виды информации могут требовать применения существенно различ-

ных алгоритмов шифрования. Следовательно, формат ESP может претерпевать значительные изменения в зависимости от используемых криптографических алгоритмов. Получатель пакета ESP расшифровывает заголовок и использует параметры и данные применяемого алгоритма шифрования для декодирования информации транспортного уровня.

Рис. 1 Архитектура IPSec

Различают два режима применения ESP и AH (а также их комбинации) - транспортный и туннельный.

Транспортный режим

Транспортный режим используется для шифрования поля данных IP пакета, содержащего протоколы транспортного уровня (TCP, UDP, ICMP), которое, в свою очередь, содержит информацию прикладных служб. Примером применения транспортного режима является передача электронной почты. Все промежуточные узлы на маршруте пакета от отправителя к получателю используют только открытую информацию сетевого уровня и, возможно, некоторые опциональные заголовки пакета (в IPv6). Недостатком транспортного режима является отсутствие механизмов скрытия конкретных отправителя и получателя пакета, а также возможность проведения анализа трафика. Результатом такого анализа может стать информация об объемах и направлениях передачи информации, области интересов абонентов, расположение руководителей.

Туннельный режим

Туннельный режим предполагает шифрование всего пакета, включая заголовок сетевого уровня. Туннельный режим применяется в случае необходимости скрытия информационного обмена организации с внешним миром. При этом адресные поля заголовка сетевого уровня пакета, использующего туннельный режим, заполняются межсетевым экраном организации и не содержат информации о конкретном отправителе пакета. При передаче информации из внешнего мира в локальную сеть организации в качестве адреса назначения используется сетевой адрес межсетевого экрана. После расшифровки межсетевым экраном начального заголовка сетевого уровня пакет направляется получателю.

Security Associations

Security Association (SA) – это соединение, которое предоставляет службы обеспечения безопасности трафика, который передаётся через него. Два компьютера на каждой стороне SA хранят режим, протокол, алгоритмы и ключи, используемые в SA. Каждый SA используется только в одном направлении. Для двунаправленной связи требуется два SA. Каждый SA реализует один режим и прото-

кол; таким образом, если для одного пакета необходимо использовать два протокола (как, например, AH и ESP), то требуется два SA.

Политика безопасности

Политика безопасности хранится в SPD (База данных политики безопасности). SPD может указать для пакета данных одно из трёх действий: отбросить пакет, не обрабатывать пакет с помощью IPSec, обработать пакет с помощью IPSec. В последнем случае SPD также указывает, какой SA необходимо использовать (если, конечно, подходящий SA уже был создан) или указывает, с какими параметрами должен быть создан новый SA.

SPD является очень гибким механизмом управления, который допускает очень хорошее управление обработкой каждого пакета. Пакеты классифицируются по большому числу полей, и SPD может проверять некоторые или все поля для того, чтобы определить соответствующее действие. Это может привести к тому, что весь трафик между двумя машинами будет передаваться при помощи одного SA либо отдельные SA будут использоваться для каждого приложения, или даже для каждого TCP соединения.

Использование отечественных стандартов шифрования

Протокол IPSec не определяет жестко, какие методы шифрования должны использоваться для аутентификации и создания защищенного канала. Методы аутентификации, типы ключей (симметричные или асимметричные), алгоритмы распределения ключей и алгоритмы шифрации могут использоваться любые. В частности, для России существующий набор алгоритмов может быть расширен алгоритмами ГОСТ 28147- 89 и ГОСТ Р 34.10/11-94.

Ни в одной из существующих реализаций протокола IPSec для Linux эти алгоритмы не реализованы, что ограничивает внедрение и использование протокола.

Для решения поставленных целей был реализован пакет ПО для операционной системы Linux. Он состоит из следующих компонентов: модуль ядра, реализующий протоколы IPSec; утилита администрирования. Модуль ядра можно функционально разделить на две части: поддержка AH и поддержка ESP. В настоящее время реализован протокол ESP и идет работа над реализацией AH. Каждый из протоколов подразумевает реализацию двух подсистем: одна для исходящих пакетов, другая для входящих. Кроме того, в модуле предусмотрена поддержка SPD, позволяющая гибко настраивать политики безопасности.

Реализация ядра системы в виде модуля ОС Linux позволила повысить защищенность системы. Это обусловлено тем, что процессы не имеют доступа к данным модуля и никакая часть адресного пространства не может быть выгружена в файл подкачки. Таким образом, исключается возможность какого-либо нежелательного влияния на функционирование модуля.

Управление осуществляется утилитой администрирования, доступ к которой имеет только системный администратор. Администратору позволено редактировать базу SPD, добавлять новые виртуальные сети (туннели), управлять ключами криптографических алгоритмов, а также отключать протоколы IPSec.

Заключение

Пакет ПО защиты сетевого трафика на основе IPSec может быть использован в любой операционной системе семейства Linux, в которой установлено одно из ядер линейки 2.4.

Как уже было отмечено ранее, на настоящий момент реализован протокол ESP, поддержка базы SPD и отечественные криптографические алгоритмы. В процессе реализации находится протокол AH.