РЕФЕРАТ

Работа посвящена анализу безопасности установления соединений в сетях IP-телефонии.

Пояснительная записка состоит из 108 страниц, 17 рисунков и 2 таблиц.

Перечень ключевых слов: аутентификация, авторизация, аудит, IP-телефония, протокол RADIUS, протокол TACACS+, протокол IPSec, Softswitch.

В работе проводится анализ безопасности установления соединения в сети IP-телефонии. Производится обзор типов угроз и возможностей различных протоколов IP-телефонии (H.323, MGCP, SIP, OSP и т.д.) с точки зрения обеспечения безопасности соединений. Приводится сравнение двух наиболее популярных протоколов аутентификации RADIUS и TACACS+, делается оценка в пользу протокола RADIUS и анализируются алгоритмы, заложенные в нем с целью обеспечения безопасности соединения. Выработана рекомендация по обеспечению безопасности соединения в сетях IP-телефонии, а также приведен сценарий работы безопасного VoIP-соединения. В работе проводится параллель между выделенными каналами сети IP-телефонии и каналами VPN. С точки зрения обеспечения информации в канале предлагается использовать технологию виртуальных частных сетей, и производится в связи с этим обзор протокола IPSec.

Основные практические результаты работы – внедрение эффективных мер обеспечения безопасности на сегодняшний день является одним из приоритетных направлений в отрасли связи.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время наблюдается бурное развитие сети Интернет, других сетей, основанных на протоколе IP, в том числе сетей IP – телефонии. Глобальная сеть Интернет прочно входит в жизнь людей, предоставляя множество услуг: от новостей и почты до многопользовательских конференций и виртуальных магазинов.

На данном этапе трудно представить успешную работу какой-либо организации, использующей компьютерную технику для ведения своих дел, без локальной сети. Крупные компании создают свои сети, располагающиеся в нескольких зданиях или даже городах.

Сегодня трудно переоценить значение информации и значение обеспечения ее безопасности. Ведь для того, чтобы заполучить важные сведения, взломщику уже нет необходимости физического доступа к ней, как это было раньше. При определенных знаниях, навыках и обладая комплексом современных программно-аппаратных средств, можно осуществить хищение (или копирование) важной информации не выходя из дома.

IP-телефония, будучи результатом слияния технологий обычной телефонии с коммутацией каналов и пакетных IP-сетей, впитала в себя и совокупность их проблем с точки зрения обеспечения безопасности. От обычной телефонии ей, прежде всего, досталась кража сервиса (правда с известными поправками), а от IP-сетей все разнообразие атак компьютерного мира: от DoS-атак на диспетчеры сети IP-телефонии до перехвата информационных пакетов с целью прослушивания или модификации.

Все многообразие угроз сетям IP-телефонии в конечном счете можно разделить на две группы: угрозы, возникающие в результате несанкционированного доступа к ресурсам сети и угрозы, связанные с передачей информации непосредственно по каналам. Для решения проблем первой группы необходим, прежде всего, устойчивый к взлому механизм аутентификации, авторизации и учета. Другие проблемы способен в какой-то мере на первый взгляд разрешить верно подобранный алгоритм шифрования

или даже некая концепция построения всей сети IP-телефонии, способная в частности реализовать данный алгоритм шифрования.

В работе определяется один из вариантов построения современной безопасной VoIP-сети, приводится анализ типов угроз и конкретные решения как с ними бороться. Как результат, производится выработка рекомендации по обеспечению безопасности в сетях IP-телефонии и дается сценарий безопасного VoIP-соединения.

Структура и состав работы:

Работа разбита на четыре главы.

В первой главе даётся краткое описание принципов технологии VoIP, вариантов построения сетей IP-телефонии. Освещаются общие проблемы информационной безопасности и приводится обзор типов угроз в сетях IP-телефонии.

Во второй главе представляется один из вариантов создания современной VoIP-сети на базе программного коммутатора Softswitch, а также дается анализ возможностей протоколов IP-телефонии с точки зрения безопасности функционирования сети.

В третьей главе производится анализ обеспечения безопасности с точки зрения проверки прав доступа к ресурсам (AAA), дается обзор протоколов TACACS+ и RADIUS, приводится сравнение их возможностей и делается вывод в пользу использования в сетях IP-телефонии протокола RADIUS. Кроме того производится выработка рекомендации по обеспечению безопасности соединения в сетях IP-телефонии и приводится сценарий работы безопасного VoIP-соединения.

В четвёртой главе производится анализ обеспечения безопасности передачи голосового трафика в канале сети IP-телефонии, на основании чего предлагается использование механизмов виртуальных частных и дается обзор протокола IPSec.

1. Анализ подхода к построению сети IP-телефонии

1.1. Общие сведения об IP-телефонии

IP-телефония - это технология, которая связывает мир телефонии и мир Интернет. До недавнего времени сети с коммутацией каналов (телефонные сети) и сети с коммутацией пакетов (IP-сети) существовали практически независимо друг от друга и использовались для различных целей. Телефонные сети использовались только для передачи голосовой информации, а IP-сети - для передачи данных. Технология IP-телефонии объединяет эти сети посредством устройства, называемого шлюз или gateway. Шлюз представляет собой устройство, в которое с одной стороны включаются телефонные линии, а с другой стороны - IP-сеть (например, Интернет).

1.1.1. История становления и перспективы развития

Существует мнение, что концепция передачи голоса по сети с помощью персонального компьютера зародилась в Университете штата Иллинойс (США). В 1993г. Чарли Кляйн выпустил в свет первую программу для передачи голоса по сети с помощью ПК.

В феврале 1995г. израильская компания VocalTec предложила первую версию программы Internet Phone, разработанную для владельцев мультимедийных PC, работающих под операционной системой Windows. Это стало важной вехой в развитии Интернет-телефонии. VocalTec надеялась использовать очень популярные (текстовые) каналы Internet Relay Chat (IRC) в качестве двустороннего средства общения между людьми. Была достигнута договоренность с компанией Eris Free Network, курирующей IRC, и создана частная сеть серверов Internet Phone, позволившая начать общаться через Интернет тысячам людей.

В том же 1995г. другие компании очень быстро оценили перспективы, которые открывала возможность разговаривать, находясь в разных

полушариях и не платя при этом за международные звонки. На рынок обрушился поток продукции, предназначенной для телефонии через Интернет.

В сентябре того же года в розничной торговле появилась первая из таких программ – DigiPhone, разработанная небольшой компанией в Далласе, которая предложили «дуплексные» возможности, позволяя говорить и слушать одновременно. Вот в этот момент и родилась привлекательная для абонентов настоящая интерактивная связь.

В марте 1996г. было объявлено о совместном проекте под названием «Internet Telephone Gateway» двух компаний: уже упоминавшейся VocalTec и крупнейшего производителя программного обеспечения для компьютерной телефонии Dialogic. Целью было «научить» работать через Интернет обычный телефонный аппарат, для чего между сетью Интернет и ТФОП устанавливался специализированный шлюз. Последний получил название VTG (VocalTec Telephone Gateway) и представлял собой специализированную программу, которая использовала голосовые платы Dialogic как интерфейс с обычными телефонными линиями. Многоканальные голосовые платы позволяли, во-первых, одной системе VTG поддерживать до восьми независимых телефонных разговоров через сеть Интернет, а во-вторых, убрали проблему адресации, взяв на себя преобразование обычных телефонных номеров в IP-адреса (и обратно). Для разговора одного пользователя в том продукте достаточно было ширины полосы канала порядка 11 кбит/с (у современных продуктов она бывает другой). Вот так возможность высокого уплотнения канала и малая стоимость связи создали предпосылки для коренных изменений телекоммуникационного мира.

К настоящему времени уже сотни компаний предложили свои коммерческие решения для IP-телефонии. Одновременно почти все крупные телекоммуникационные компании, использующие традиционные средства для организации телефонных переговоров, почувствовали угрозу рынку

предоставляемых ими услуг, начали интенсивные исследования с целью оценки ее реальности и масштаба.

По прогнозам компании Yankie Group, доля междугородных и международных звонков (по времени), осуществляемых по IP-сетям, имеет большую тенденцию роста и достигнет, например, в США к 2005г. 15%. В то же время, по оценкам компании TeleChoice через пять лет доля рынка IP-телефонии возрастет всего лишь до 2%.

Независимо от приведенных прогнозов с уверенностью можно сказать, что IP-телефония в ближайшее время не станет полноценной альтернативой традиционной телефонии, но сможет занять определенное место особенно в корпоративном сегменте, где в полной мере проявит свое истинное преимущество – возможность сопровождения телефонными переговорами потока данных в едином канале связи. Сеансы одновременной работы с одной и той же информацией в корпоративных сетях, видеоконференции, Интернет-коммерция в режиме «он-лайн» - вот где IP-телефония несомненно займет достойное положение даже с пониженным качеством речи, поскольку основную смысловую нагрузку в этих случаях будет нести информация на дисплее компьютера или видеоэкране.

Провайдерам Интернет и операторам телефонной связи введение IP-телефонии в спектр услуг открывает совершенно новые рынки сбыта, новых клиентов и возможности развития.

Корпоративным клиентам - многократное снижение затрат на междугородние (международные) переговоры, организация виртуальных частных сетей между удаленными филиалами, звонок из Интернета на корпоративном Web-сайте.

Интернет-магазинам и каталогам - Web-телефон

Частным пользователям - многократное снижение затрат на междугородние (международные) переговоры, все услуги связи от одного

оператора, роуминг по городам России и Мира, звонок с компьютера, звонок с Web-сайта.

1.1.2. Преимущества IP-телефонии

С точки зрения конечного пользователя, он не только сохранит имеющиеся преимущества телефонной сети общего пользования, которые включают широкий диапазон услуг, простоту использования, надежность и качество голоса, но и получит следующие дополнительные преимущества:

- Более низкие цены на традиционные услуги телефонной связи;
- IP-телефония одновременно поддерживает голос и данные, удовлетворяя требованиям конвергенции. Это означает, что клиенты получат дополнительные преимущества от экономии в развитии, возможные за счет использования единой сети;
- Феноменальная мобильность пользователя, которую обеспечивает сеть IP-телефонии: звонки и факсы автоматически перенаправляются в любую точку мира, пользователи будут иметь доступ к одному и тому же набору услуг вне зависимости от того, где и как они подключаются к сети;
- Новый набор устройств доступа, от традиционных телефонов и факсов до компьютеров;
- Доступ к новым услугам (голосовая почта, конференцсвязь, передача факса и др.) через открытый интерфейс архитектуры на базе IP, что обеспечивает совместимость для широкого спектра разработчиков приложений;
- Возможность настройки набора услуг;
- Простота оплаты услуг IP-телефонии (в частности с помощью предоплаченных телефонных карт);
- Простота контроля пользователем состояния его расчетного счета (обычно через web-интерфейс).

Кроме того, к сети IP-телефонии применимы все те же методы и технологии обеспечения отказоустойчивости, что и в обычной компьютерной сети. Также существуют специальные методы по сохранению резервной телефонной связи в случае потери сообщения между удалённым офисом и центром коммутации телефонных вызовов.

Наряду с провайдерами IP-телефонии Интернет-провайдеры также могут занять определенную нишу на рынке услуг IP-телефонии, так как существующая у них IP-инфраструктура дает хорошие возможности для внедрения услуг голосовой связи. Необходимые для этого аппаратные и программные средства можно устанавливать поэтапно. Интернет-провайдеры уже имеют точки присутствия, связанные с коммутаторами местных провайдеров и операторов сети общего пользования.

Для Интернет-провайдеров услуга Интернет-телефонии обеспечивает следующие преимущества:

- Сбережение капитальных вложений за счет использования открытых компьютерных платформ;
- Снижение эксплуатационных расходов как результат предоставления разнообразия услуг на базе единой сети;
- IP-сети основаны на ряде универсальных глобальных стандартов, что позволяет многим производителям предлагать свои продукты. Благодаря этим стандартам, стала возможна открытая конкуренция многочисленных производителей аппаратного обеспечения и провайдеров сетевых служб. Конкуренция приводит к снижению цен и расширяет спектр услуг для конечного пользователя;
- Множество услуг может быть доступно через единственный канал с пользователем, что означает больше услуг (прибыли) в расчете на одного пользователя.

Тем не менее, оказывается, что, к сожалению, IP-телефония, не приводит к многократной экономии средств оператора, вкладываемых в передачу голосового трафика на дальние расстояния, как это на первый взгляд может показаться при анализе деятельности сегодняшних компаний, предоставляющих эти услуги. И камнем преткновения здесь является все то же качество передачи речи. В результате сегодня IP-технологии с успехом применяются для создания выделенных мультисервисных сетей связи. Для гарантии качества при передачи трафика на дальние расстояния вместо каналов общедоступного Интернета нужны выделенные магистральные каналы (хотя и уплотненные с помощью технологии IP-телефонии) во все требуемых регионы и страны, нужна более мощная местная телефонная сеть в местах установки шлюза (для этого нужно вкладывать в местную сеть ТФОП инвестиции) и так далее. Именно так и работают сегодня серьезные поставщики услуг IP-телефонии. Таким образом, для крупных операторов IP-телефония сегодня – это способ более эффективно использовать существующий сетевой ресурс и возможность предоставления своим клиентам современного спектра дополнительных услуг, которые не реализуемы в традиционной сети, и за счет которых оператор может получить дополнительную прибыль.

1.1.3. Варианты построения сетей IP-телефонии

Наиболее известным является подход, предложенный Международным союзом электросвязи (ITU) в Рекомендации H.323. Сети, построенные на базе протоколов H.323, ориентированы на интеграцию с телефонными сетями и могут рассматриваться как наложенные на сети передачи данных сети ISDN. В частности, процедура установления соединения в таких сетях IP-телефонии базируется на Рекомендации ITU Q.931 и практически идентична данной процедуре в сетях ISDN.

Описанный вариант построения сетей IP-телефонии больше подходит для операторов телефонной связи, желающих использовать сети с маршрутизацией пакетов IP для предоставления услуг междугородной и международной связи.

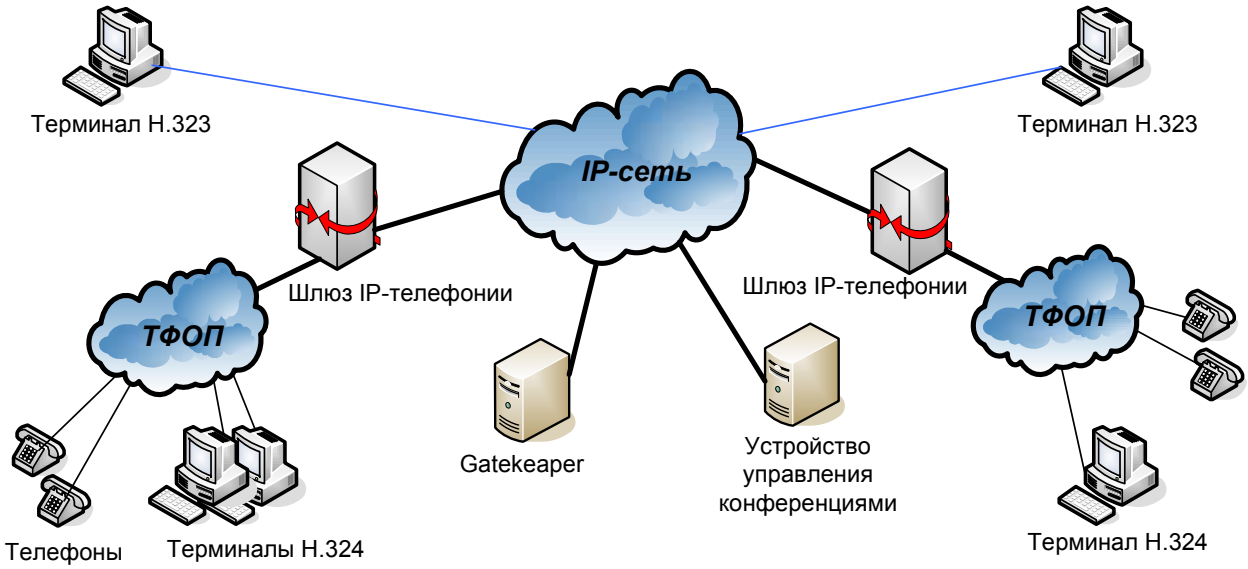


Рис. 1.1. Архитектура сети, базирующейся на протоколе H.323

Причем IP-телефония будет для них основной предоставляемой услугой. Протокол RAS, входящий в набор протоколов H.323, обеспечивает операторам связи высокий уровень контроля за использованием сетевых ресурсов, поддержку аутентификации пользователей и начисление оплаты за предоставленные услуги. Кроме базового вызова в сетях, построенных на базе протоколов H.323, предусмотрено предоставление дополнительных услуг в соответствии с Рекомендациями ITU H.450.x.

Второй подход, связанный с использованием протокола SIP (Session Initiation Protocol), ориентирован на интеграцию услуги передачи речевого трафика по IP-сетям с остальными услугами Internet. Этот подход, предложенный телекоммуникационной стандартизирующей организацией IETF в документе RFC 2543, является намного более простым для реализации

в сравнении с H.323, но меньше подходит для организации взаимодействия с телефонными сетями. В основном это связано с тем, что сервер SIP не сохраняет сведений о текущих соединениях (Stateless), то время как узлы ТфОП напротив сохраняют информацию обо всех установленных соединениях (Statefull). Кроме того, сигнальный протокол SIP, базирующийся на основе протокола HTTP (RFC 2068), плохо согласуется с системами сигнализации, используемыми в ТфОП.

Этот вариант больше подходит для поставщиков услуг Интернет для предоставления еще одной услуги - Интернет-телефонии. Причем эта услуга будет являться всего лишь небольшой частью пакета услуг, и будет предоставляться, например, по фиксированным тарифам, при этом будет использоваться максимально упрощенная схема управления услугами.

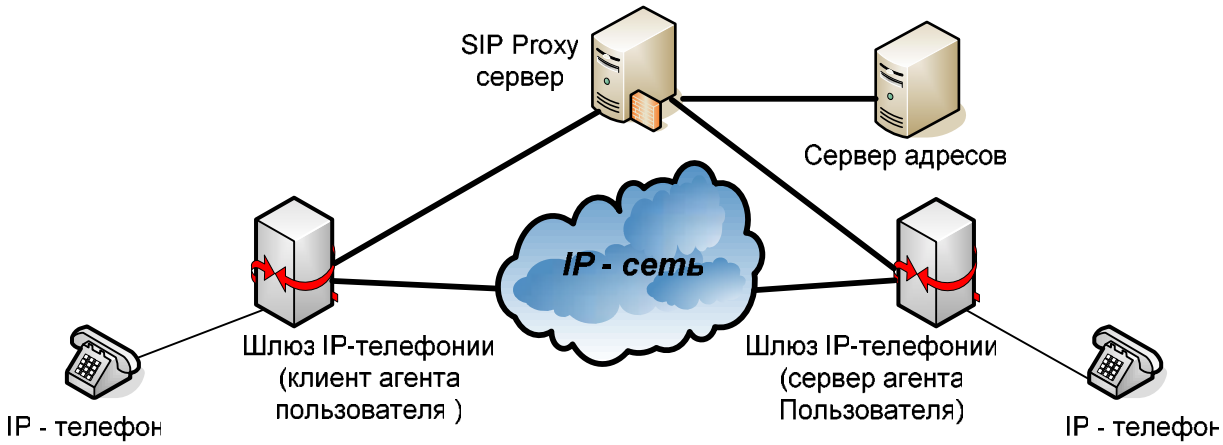


Рис.1.2. Архитектура сети, базирующейся на протоколе SIP

Еще один подход, связанный с декомпозицией шлюзов, предполагает разбиение шлюзов на основные функциональные блоки: шлюз - MG (Media Gateway), устройство управления шлюзом - CA (Call Agent) и сигнальный шлюз - SG (Signalling Gateway), и определение интерфейсов между блоками. Весь интеллект декомпозированного шлюза: обработка сигнальной информации и логика контроля ресурсов - сосредоточен в устройстве управления. Сами шлюзы только выполняют функции преобразования речевой

информации, поступающей со стороны ТФОП в вид пригодный для передачи по сетям с маршрутизацией пакетов IP: кодирование и упаковка речевой информации в пакеты RTP/UDP/IP, а также обратное преобразование. Один контроллер шлюзов CA управляет одновременно несколькими шлюзами. Сигнальный шлюз выполняет функции STP . транзитного пункта сигнализации. Такое решение обеспечивает высокую степень масштабируемости и простоту эксплуатации сети. Шлюзы не являются интеллектуальными устройствами, требуют меньшей производительности процессоров и, следовательно, становятся менее дорогими. Кроме того очень быстро вводятся новые протоколы сигнализации или дополнительные услуги, так как эти изменения затрагивают только контроллер шлюзов, а не сами шлюзы. Третий подход, предлагаемый организацией IETF (рабочая группа MEGACO) достаточно хорошо подходит для развертывания глобальных сетей IP-телефонии, приходящих на смену традиционным телефонным сетям. Если распределенный шлюз подключается к ТФОП при помощи сигнализации по выделенным сигнальным каналам (ВСК), то сигнальная информация вместе с пользовательской информацией сначала поступает в транспортный шлюз, а затем передается в устройство управления без посредничества шлюза сигнализации. Одно из основных требований, предъявляемых к протоколу MGCP, состоит в том, что устройства, реализующие этот протокол, должны работать в режиме без сохранения информации о последовательности транзакций между устройством управления и транспортным шлюзом, т.е. в устройствах не требуется реализации конечного автомата для описания этой последовательности. Однако не следует распространять подобный подход на последовательность состояний соединений, сведения о которых хранятся в устройстве управления.

Отметим, что протокол MGCP является внутренним протоколом, поддерживающим обмен информацией между функциональными блоками распределенного шлюза. Протокол использует принцип master/slave

(ведущий/ведомый), причем устройство управления шлюзами является ведущим, а транспортный шлюз – ведомым, выполняющим команды, поступающие от устройства управления.

Подход на базе протокола MGCP обладает очень важным преимуществом перед подходом, предложенным ITU в Рекомендации H.323: поддержка управляющим устройством сети - CA сигнализации ОКС7 и других видов сигнализации, а также прозрачная трансляция сигнальной информации по сети IP-телефонии. В H.323 сигнализация ОКС7, как и любая другая сигнализация, конвертируется шлюзом в сигнальные сообщения H.225.0 (Q.931).

Основным недостатком последнего подхода является незаконченность стандартов. Функциональные составляющие декомпозированных шлюзов, разработанные различными фирмами-производителями телекоммуникационного оборудования, практически не совместимы. Функции управляющего устройства - CA точно не определены. К недостаткам можно также отнести отсутствие стандартизированного протокола взаимодействия между CA. Кроме того, протокол MGCP является протоколом управления шлюзами, но он не предназначен для управления соединениями с участием терминального оборудования пользователей (IP-телефонами). Это означает, что в сети, построенной на базе протокола MGCP, должен присутствовать Привратник или сервер SIP для управления терминальным оборудованием.

Стоит также отметить, что в существующих приложениях IP-телефонии: таких как предоставление услуг международной и междугородной связи, использовать протокол MGCP не целесообразно, в связи с тем, что подавляющее количество систем IP-телефонии сегодня построено на базе протокола H.323. Оператору придется строить отдельную сеть IP-телефонии, построенную на базе протокола MGCP, что связано со значительными капиталовложениями. В то время как, оператор связи, имеющий оборудование стандарта H.323, может подключиться к существующим сетям IP-телефонии.

Стоит также отметить, что в проекте Рекомендации H.323, версии 4 ITU ввел принцип декомпозиции шлюзов, описанный в последнем подходе.

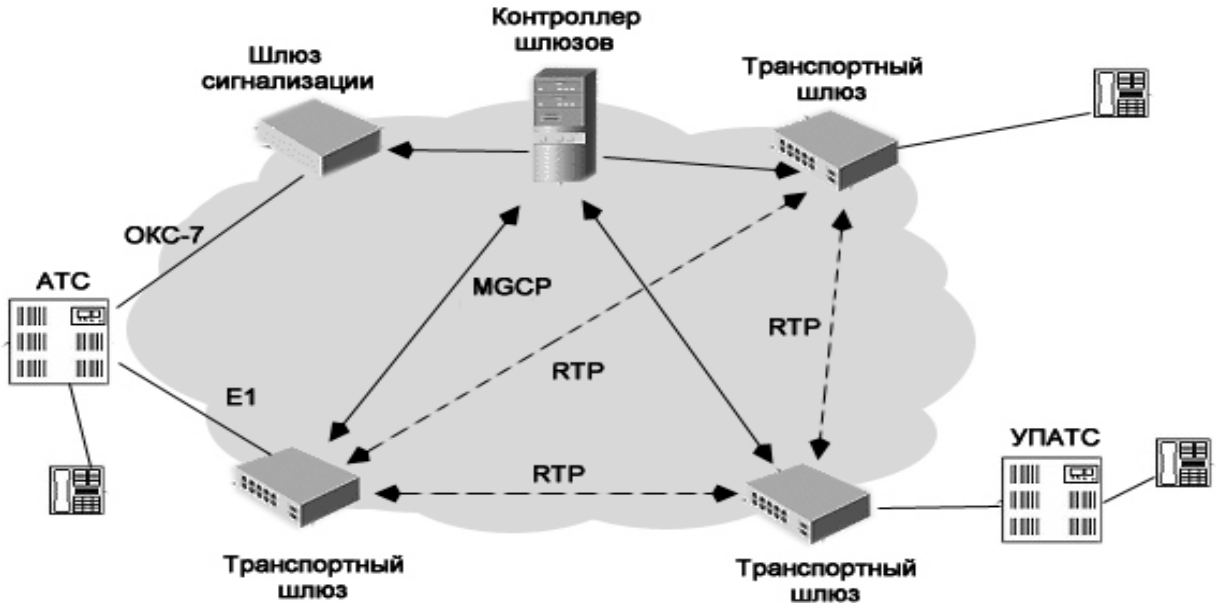


Рис.1.3. Архитектура сети, базирующейся на протоколе MGCP

Управление функциональными блоками декомпозированного шлюза будет осуществляться контроллером шлюза - MGC (Media Gateway Controller) при помощи протокола H.248, который пока еще не утвержден ITU, но уже сегодня превосходит протокол MGCP по своим возможностям. Европейский телекоммуникационный институт стандартизации ETSI (рабочая группа TIPHON) также предусмотрел интеграцию принципа декомпозиции шлюза с протоколами H.323.

Также в проекте Рекомендации H.323, версии 4 предусмотрена возможность прозрачной передачи сигнализации ОКС7 и других видов сигнализации по сетям IP-телефонии и обработка всех видов сигнализации Привратником без преобразования в сигнальные сообщения H.225.0.

Выше указанное означает, что Рекомендация H.323 вбирает в себя все самое лучшее, что предлагается в альтернативных подходах к построению сетей IP-телефонии. Кроме того, поддержка Привратником сигнализации

ОКС7 обеспечивает возможность развертывания Интеллектуальных сетей связи (ИС) на базе сетей IP-телефонии.

1.1.4. Основные принципы построение сети H.323

Для того, чтобы предоставлять услуги IP-телефонии по dial-up, как минимум необходимо установить станционный шлюз, к которому подключаются телефонные линии городской АТС . Шлюз настраивается на оборудование оператора IP-телефонии. Клиенту предоставляется городской телефонный номер, и уникальный персональный код доступа (PIN.

Шлюзы и объединяющая их IP-сеть являются необходимыми элементами для построения телефонной пакетной сети, однако на практике в состав операторского решения входит немало и других компонентов — контроллеры домена или привратники (gatekeeper), система биллинга, и т. п. Они не входят в число обязательных элементов сети, но существенно облегчают жизнь операторам.

1.1.4.1. Шлюз

Шлюз представляет собой связующее звено между телефонной сетью общего пользования и сетью с коммутацией пакетов, обеспечивает стандартный интерфейс для связи с ТФОП, преобразует речевые и факсимильные сигналы используя алгоритмы кодирования/декодирования (кодеки) из формата коммутации каналов в формат коммутации пакетов и обратно. Он работает с gatekeeper-ом по протоколу RAS для маршрутизации вызовов в сети.

С телефонной сетью общего пользования или учрежденческой связи шлюзы IP-телефонии взаимодействуют через интерфейс телефонной линии или ISDN. Цифровой сигнальный процессор (Digital Signal Processor, DSP) осуществляет, когда это необходимо, демультиплексирование (в случае линий T-1/E-1) и оцифровывание (в случае аналоговых линий), сжатие и кодирование речи и

передачу упакованной речи дальше в сеть. Благодаря универсальности протокола IP, т. е. его способности использовать в качестве транспорта практически все что угодно, это может быть интерфейс Ethernet, Token Ring, ATM, SDH и т. д. Таким образом, шлюз IP-телефонии выполняет следующие пять основных функций:

- функции интерфейса с УАТС, телефонной сетью общего пользования и другими телефонными сетями;
- базовые функции обслуживания вызовов (соединение/разъединение и т. п.);
- компрессию и декомпрессию речи в реальном времени;
- упаковку и распаковку сжатой речи;
- функции интерфейса с сетью IP.

Шлюз, в совокупности с привратником сети IP-телефонии, образует универсальную платформу для предоставления всего спектра услуг IP-телефонии.

1.1.4.2. Привратник (gatekeeper)

Использование привратника повышает возможности масштабирования, за счет централизации данных о маршрутах и планах нумерации, что облегчает процессы модификации и расширения сети. Привратник работает с адресной системой, определяет IP адреса удаленного шлюза, указанного в конфигурации для вызываемого номера. Данное устройство также управляет полосой пропускания и качеством услуг. Каждый привратник имеет понятие "зоны" административного контроля, в пределах которой он управляет множеством шлюзов. Такие зоны, как правило, устанавливаются соответственно границам географических зон. Привратник управляет маршрутизацией сигнальных сообщений между терминалами, расположенными в одной зоне: привратник может организовывать сигнальный канал напрямую между терминалами или же ретранслировать сигнальные

сообщения от одного терминала к другому. В этом случае привратник в любое время знает состояние конечных пользователей, поэтому на него может возлагаться предоставление дополнительных услуг: переадресация, передача, постановка на ожидание и перехват вызова и т.д.

При отсутствии в сети привратника, преобразование адреса вызываемого абонента в транспортный адрес IP-сети должно выполняться шлюзом.

1.1.4.3. Серверы биллинга

Серверы биллинга используются для проведения расчетов за предоставляемые оператором услуги связи. Для того, чтобы не использовать различные биллинговые системы для учета различных услуг, лучше всего остановиться на биллинговых системах нового типа, позволяющих учитывать все современные услуги связи.

RADIUS сервер выполняет функции идентификации, авторизации и учета (AAA). Сервер RADIUS собирает и сохраняет данные о вызовах, которые поступают от шлюзов VoIP. Серверы биллинга собирают эти данные с серверов RADIUS и обрабатывают данные с помощью специальных биллинговых приложений. Счета рассылаются абонентам через Интернет или по почте в зависимости от модели обслуживания, принятой у того или иного провайдера.

1.2. Информационная безопасность

1.2.1. Общие положения и определения

Действующим ОСТ 45.127-99 «Система обеспечения информационной безопасности Взаимоувязанной сети связи Российской Федерации. Термины и определения » введены следующие ключевые понятия:

- *Информационная безопасность сети* - состояние защищенности информационной сферы сети от заданного множества угроз;

- *Система обеспечения информационной безопасности сети*, далее система защиты, - совокупность правовых норм, технических мероприятий и механизмов защиты, направленных на противодействие заданному множеству угроз информационной безопасности сети;
- *Политика информационной безопасности* – система мероприятий, направленных на обеспечение информационной безопасности.

Кроме того, определим ряд понятий, которые неоднократно будем использовать в ходе данной дипломной работы:

- *Аутентификация* – процесс проверки какого-либо идентификатора из известного пространства имен. В случае оператора IP-телефонии – проверки номера карты и пин-кода.
- *Авторизация* – процесс проверки пользователя на предмет возможности использования какого-либо ресурса.
- *Аудит* – процесс учета используемого сервиса.
- *Хэш-функции* – функции, отображающие сообщения произвольной длины в значения фиксированной длины, которые часто называют хэш-кодами.

Необходимость знания возможных угроз, способных привести к необратимым последствиям в функционировании сети в целом, очевидна. Перечень угроз и их классификация, в сочетании с оценкой вероятности реализации конкретной угрозы, служат основой для анализа риска реализации угроз и формулирования требований к системе защиты. Конечной целью классификации угроз является выбор эффективных средств противодействия при издержках на систему информационной безопасности не превосходящих стоимость потерь, ожидаемых от реализации угроз.

Необходимо оговорить еще один важный момент, заключающийся во внутреннем противоречии решаемых задач. Он состоит в том, что задачи, которые решает система защиты с точки зрения производителя всегда состоят в противоречии с задачами, которые она должна решать с точки зрения

интересов пользователя. Нахождение «золотой середины» для снятия данного противоречия не всегда является рациональным. Достижение необходимого баланса должно осуществляться для каждого частного случая за счет гибкости самой системы защиты.

1.2.2. Атаки на операторов связи

О необходимости наличия эффективных механизмов обеспечения безопасности в сетях операторов связи говорят следующие примеры. CloudNine Communications, один из самых старейших британских Internet-провайдеров, был атакован злоумышленниками в конце января 2002г. Против него были реализованы уже ставшие классикой распределенные атаки "отказ в обслуживании" (DDoS).

CloudNine, компания с шестилетним стажем, была вынуждена завершить свой бизнес и продать базу данных всех своих клиентов своему конкуренту - компании Zetnet. Атака была грамотно спланированной акцией, которая продолжалась не один месяц. В течение длительного времени злоумышленники собирали информацию о ключевых серверах и их пропускной способности. В решающий момент был нанесен удар, от последствий которого так и не удалось оправиться.

Незадолго до атаки на CloudNine был зафиксирован ряд атак и на других провайдеров. Например, в конце января 2002г. также пострадали портал британского представительства итальянского ISP Tiscali и британский ISP Donhost. Первый не мог работать в течение нескольких дней, а функционирование второго было нарушено на нескольких часов. Эти атаки затрагивают доходы компаний, т.к. пользователи не могут получить доступ к предоставляемым услугам. Это очень сильный удар по бизнесу.

При этом обнаружить злоумышленников, которые задействовали сотни узлов для своей атаки и могли подготовить плацдарм задолго до осуществления ее, практически невозможно.

Вследствие DDoS-атак в феврале 2002 года была нарушена нормальная работа многих провайдеров, в том числе SniffOut, TheDotComplete, The DogmaGroup, Firenet и т.д. Надо сказать, что атаки начались задолго до 2002 года. Например, 7 и 14 декабря 1996 года Web-сервер американского Internet-провайдера Web Communications LLC был выведен из строя на и 9 и 40 часов соответственно. Эта атака, получившая название SYN Flood, нарушила деятельность более 2200 корпоративных клиентов Web Communications. Не проходит месяца, чтобы не была зафиксирована атака на операторов связи во всем мире.

По данным России-Онлайн в течение двух суток в 2000 г. крупнейший Internet-провайдер Армении "Арминко" подвергался распределенной атаке, в которой участвовало более 50 машин из разных стран. Хотя атаке подверглась в основном "Арминко", перегруженной оказалась вся магистраль, соединяющая Армению с всемирной паутиной.

Как же защититься от такого рода атак? Первое - применить списки контроля доступа маршрутизаторов или использовать межсетевые экраны. Именно так и делает абсолютное большинство провайдеров. Но эффективен ли такой метод? Лишь отчасти. Даже при использовании межсетевых экранов и задействованных списках контроля доступа на маршрутизаторах с распределенными атаками крайне трудно справиться. Какие еще способы существуют? Самый просто способ - это своевременно отслеживать все новые способы DoS-атак и, особенно, их распределенных модификаций, чтобы своевременно противопоставить им соответствующие защитные механизмы.

Если перейти к техническим мерам защиты, то к ним, помимо межсетевых экранов и списков контроля доступа, можно отнести применение сканеров безопасности и систем обнаружения атак. Эти средства достаточно подробно описаны в различных специализированных источниках. Отметим только, что существующие системы обнаружения атак уже лишены одного из главных недостатков - низкой скорости работы. На сегодняшний день есть решения,

которым "по плечу" 100 Мбит/сек и даже выше. Например, модуль CiscoSecure Catalyst 6000 IDS Module, который расширяет функциональность коммутаторов Catalyst серии 6000 за счет обнаружения атак. Общая производительность такой платы, вставляемой в шасси Catalyst'a, составляет около 200 Мбит/сек. Если говорить о программных решениях, то можно назвать самую первую систему обнаружения атак, поддерживающая гигабитный трафик - RealSecure Gigabit Sentry компании Internet Security Systems. Существует и "суррогатное" решение, заключающееся в распараллеливании гигабитного трафика среди нескольких систем обнаружения атак. Устройство, осуществляющее такую задачу, выпускает компания TopLayer Networks.

Стоит отметить еще одну защитную меру, которая реализуется уже не техническими, а организационными мерами. Это страхование информационных рисков. В качестве практического примера ее реализации приведем опыт одной из крупнейших страховых компаний Германии - концерн Gerling, которая в 1998 стала предлагать всем фирмам, занятым в сфере Internet-услуг и IP-телефонии, страхование по возмещению ущерба.

1.2.3. Типы угроз в сетях IP-телефонии

Не смотря на несомненные преимущества IP-телефонии нельзя обойти вниманием такую ее проблемную область как безопасность. IT-специалистам, включая и специалистов по защите информации, крайне желательно знать возможные угрозы компонентам инфраструктуры IP-телефонии и возможные способы защиты от них, включая и возможности существующих VoIP-стандартов с точки зрения информационной безопасности.

Зачем атакуют сеть IP-телефонии? Это хорошая цель для взломщиков. Некоторые из них могут подшутить над вами, послав вам голосовое сообщение от имени руководства компании. Кто-то может захотеть получить доступ к голосовому почтовому ящику вашего руководства или даже захочет

перехватить голосовые данные о финансовых сделках, которыми обмениваются сотрудники финансового департамента или бухгалтерии. Конкуренты могут захотеть подорвать репутацию провайдера IP-телефонии путем выведения из строя шлюзов и диспетчеров, тем самым, нарушая доступность телефонных услуг для абонентов, что, в свою очередь, может также привести к нанесению ущерба бизнесу клиентов. Существуют и другие причины, например, звонки за чужой счет (кража сервиса).

Главная проблема с безопасностью IP-телефонии в том, что она слишком открыта и позволяет злоумышленникам относительно легко совершать атаки на ее компоненты. Несмотря на то, что случаи таких нападений практически неизвестны, они могут быть при желании реализованы, т.к. атаки на обычные IP-сети практически без изменений могут быть направлены и на сети передачи оцифрованного голоса. С другой стороны, похожесть обычных IP-сетей и сетей IP-телефонии подсказывает и пути их защиты, но об этом чуть дальше.

IP-телефония, являясь прямой родственницей обычной телефонии и IP-технологии, вобрала в себя не только их достоинства, но и их недостатки. Т.е. атаки, присущие обычной телефонии, также могут быть применены и для ее IP-составляющей. Перечислим некоторые из них, часть из которых рассмотрим более подробно:

- Перехват данных (подслушивание);
- Отказ от обслуживания (Denial of Service – DoS);
- Подмена номера;
- Кража сервисов;
- Неожидаемые вызовы;
- Несанкционированное изменение конфигурации;
- Мошенничество со счетом.

Перехват данных - самая большая проблема, как обычной телефонии, так и IP-телефонии. Однако в последнем случае эта опасность намного выше, т.к. злоумышленнику уже не надо иметь физический доступ к телефонной линии.

Ситуацию ухудшает еще и тот факт, что множество протоколов, построенных на базе стека TCP/IP, передают данные в открытом виде. Например, это касается HTTP, SMTP, IMAP, FTP, Telnet и, в том числе, протоколы IP-телефонии. Злоумышленник, который смог перехватить голосовой IP-трафик (а он по умолчанию между шлюзами не шифруется) может без труда восстановить исходные переговоры. Для этого существуют даже автоматизированные средства. Например, утилита vomit (Voice Over Misconfigured Internet Telephones), которая конвертирует данные, полученные в результате перехвата трафика с помощью свободно распространяемого анализатора протоколов tcpdump, в обычный wav-файл, прослушиваемый с помощью любого компьютерного плейера. Эта утилита позволяет конвертировать голосовые данные, переданные с помощью IP-телефонов Cisco и сжатые с помощью кодека G.711. Мало того, помимо несанкционированного прослушивания злоумышленники могут повторно передать перехваченные голосовые сообщения (или их фрагменты) для достижения своих целей.

Однако стоит отметить, что перехват голосовых данных - не такая простая задача, как кажется на первый взгляд. Злоумышленник должен иметь информацию об адресах шлюзов или абонентских пунктов, используемых VoIP-протоколах (например, H.323) и алгоритмах сжатия (например, G.711). В противном случае, злоумышленнику будет трудно настроить ПО для перехвата трафика или объем перехваченных данных и время для их анализа превысит все допустимые пределы.

Перехват данных может быть осуществлен как изнутри корпоративной сети, так и снаружи. Квалифицированный злоумышленник, имеющий доступ к физической среде передаче данных, может подключить свой IP-телефон к коммутатору и таким образом подслушивать чужие переговоры. Он также может изменить маршруты движения сетевого трафика и стать центральным узлом корпоративной сети через который проходит интересующий его трафик. Причем, если во внутренней сети вы можете с определенной долей

вероятности обнаружить несанкционированно подключенное устройство, перехватывающее голосовые данные, то во внешней сети обнаружить ответвления практически невозможно. Поэтому любой незашифрованный трафик, выходящий за пределы корпоративной сети, должен считаться небезопасным.

Отказ в обслуживании

Традиционная телефонная связь всегда гарантирует качество связи даже в случае высоких нагрузок, что не является аксиомой для IP-телефонии. Высокая нагрузка на сеть, в которой передаются оцифрованные голосовые данные, приводит к существенному искажению и даже пропаданию части голосовых сообщений. Поэтому одна из атак на IP-телефонию может заключаться в посылке на сервер IP-телефонии большого числа "шумовых" пакетов, которые засоряют канал передачи данных, а в случае превышения некоторого порогового значения могут даже вывести из строя часть сети IP-телефонии (т.е. атака "отказ в обслуживании"). Что характерно, для реализации такой атаки нет необходимости "изобретать велосипед" - достаточно использовать широкие известные DoS-атаки Land, Ping of Death, Smurf, UDP Flood и т.д. Одним из решений этой проблемы является резервирование полосы пропускания, которого можно достичь с помощью современных протоколов, например, RSVP. Более подробно способы защиты будут рассмотрены далее. Отказ в обслуживании - серьезная проблема для устройств IP-телефонии. Учитывая, что загруженные сервера могут приносить огромные доходы в час, успешные атаки с организацией отказа в обслуживания приводят к серьезным финансовым потерям.

Одна из атак, которая появилась в конце 1990-х годов, получила название SYN-лавины, так как в ее основе лежало использование пакетов синхронизации, или SYN-пакетов, которые открывают TCP-соединение. Атакующая хост-машина генерирует тысячи отдельных сообщений, каждое из которых пытается начать трехэтапное квитирование по протоколу TCP.

Каждое сообщение содержит другой фиктивный адрес отправителя, так что каждое как бы собирается открыть отдельное соединение. Хост-машина – жертва пытается сгенерировать соответствующий TCP-ответ и посылает его на каждый фиктивный адрес. Она держит эти полуоткрытые соединения, ожидая ответа, который никогда не придет. Одновременно атакующая машина продолжает слать новые и новые фиктивные пакеты, запрашивая все новые и новые соединения. В конечном итоге эти полуоткрытые соединения расходуют все ресурсы хоста по соединениям, и последующие запросы на установление соединений от законных клиентов будут сбрасываться.

Хорошей защитой от подобных атак было улучшение способа обработки набором протоколов полуоткрытых соединений, в частности пересмотр работы в тех ситуациях, когда таких соединений очень много. Было предложено и реализовано несколько методов, и результаты оказались достаточно успешными. Одна стратегия заключалась в ведении списка полуоткрытых соединений в порядке поступления запросов и отбрасывании более старых при поступлении новых запросов. Хотя при возникновении лавины это могло приводить к отказу в установлении соединения для законных запросов, все же чаще подобный подход позволял устанавливать законные соединения даже во время массового поступления запросов.

Подмена номера

Для связи с абонентом в обычной телефонной сети вы должны знать его номер, а в IP-телефонии - роль телефонного номера выполняет IP-адрес. Следовательно, возможна ситуация, когда злоумышленник, используя подмену адреса, сможет выдать себя за нужного вам абонента. Или он может фальсифицировать IP-адрес с целью имитации узла, которому разрешен доступ к приложениям и сервисам, выполняющим аутентификацию запросов на основе проверки адресов. С помощью фальсификации IP-адреса внешний злоумышленник пытается представиться заслуживающим доверия узлом, находящимся внутри или вне сети. Для фальсификации выбирается IP-адрес из

диапазона IP-адресов, используемых внутри сети, или же авторизованный внешний IP-адрес, которому вы доверяете и которому разрешается доступ к определенным ресурсам сети. Фальсификация адреса обычно предполагает манипуляцию данными пакетов TCP/IP, в результате чего нарушитель получает возможность выступать от имени другого узла. Например, злоумышленник может фальсифицировать IP-адрес и представить себя в качестве легального пользователя или даже рабочей станции, чтобы получить привилегии доступа более высокого уровня. При попытке обойти механизм аутентификации, основанный на проверке адресов, он может указать для пакета произвольный адрес источника. Наибольший эффект достигается в случае, когда в качестве адреса источника внешний злоумышленник может указать адрес внутреннего узла, находящимся за маршрутизатором периметра или брандмауэром. Тогда он, используя фальсификацию IP-адреса, может обойти механизмы аутентификации, а при недостаточно квалифицированной их реализации может разрушить и фильтры на фильтрующих маршрутизаторах.

Именно поэтому задача обеспечения аутентификации не обойдена вниманием во всех существующих VoIP-стандартах и будет рассмотрена в третьей главе. Контрмерой против подобных атак является фильтрация пакетов, приходящих извне, а объявляющих себя пришедшими из самой сети. Соответствующие фильтры устанавливаются в маршрутизаторе периметра, но соответствующие атаки обнаруживаются системой обнаружения вторжений, например, CiscoSecure IDS.

Атаки на абонентские пункты

Необходимо понимать, что абонентские пункты, реализованные на базе персонального компьютера, являются менее защищенными устройствами, чем специальные IP-телефоны. Этот тезис также применим и к любым другим компонентам IP-телефонии, построенным на программной основе. Это связано с тем, что на такие компоненты можно реализовать не только специфичные

для IP-телефонии атаки. Сам компьютер и его составляющие (операционная система, прикладные программы, базы данных и т.д.) подвержены различным атакам, которые могут повлиять и на компоненты IP-телефонии. При этом, даже если в самом ПО не найдено уязвимостей (до поры до времени), то используемые им другие программные компоненты третьих фирм (особенно широко известные) могут снизить общую защищенность до нуля. Ведь давно известно общее правило - "защищенность всей системы равна защищенности самого слабого ее звена". Для примера можно привести Cisco CallManager, который использует для своего функционирования Windows 2000 Server, MS Internet Information Server и MS SQL Server, каждый из которых обладает своим набором недостатков с точки зрения обеспечения безопасности.

Атаки на узлы сети

Злоумышленники могут атаковать и узлы (Gatekeeper в терминах H.323), которые хранят информацию о разговорах пользователей (имена абонентов, время, продолжительность, причина завершения звонка и т.д.). Это может быть сделано, как с целью получения конфиденциальной информации о самих разговорах, так и с целью модификации и даже удаления указанных данных. В последнем случае биллинговая система (например, у оператора связи) не сможет правильно выставлять счета своим клиентам, что может нарушить функционирование или нанести ущерб всей инфраструктуре IP-телефонии.

2. Возможности стандартов IP-телефонии с точки зрения обеспечения безопасности

2.1. Современное видение VoIP сети

2.1.1. Мультисервисная сеть нового поколения

После того как схлынула волна всеобщей эйфории, связанной с широким распространением пакетных технологий и предсказаниями скорой гибели классических телефонных операторов, большинство аналитиков телекоммуникационного рынка пришли к мнению, что наряду с сетями, основанными на пакетных технологиях, будут еще довольно долго существовать сети с коммутацией каналов, предоставляющие классические телефонные услуги. Такой вывод позволяет сделать сравнение доходов генерируемых различными видами сетей. Несмотря на быстрый рост объемов трафика передачи данных, доходы, приносимые данным видом услуг, не скоро сравняются с доходами от телефонных услуг. Более трезвому взгляду на ситуацию способствовало и постепенное выравнивание тарифов. Из-за появления большого количества молодых активных конкурентов из мира пакетных сетей, классические телефонные операторы были вынуждены сильно понизить свои тарифы на междугородную телефонную связь, в свою очередь, крупные компании, занимающиеся передачей голосовых сообщений по пакетным сетям, пришли к необходимости значительно улучшить качество предоставляемых сервисов с целью привлечения клиентов бизнес-класса, что повысило себестоимость их услуг, а, следовательно, и тарифы. Понимание того, что операторам еще долгое время предстоит работать в условиях параллельного существования сетей, основанных на различных технологиях, привело к смене революционной модели развития на эволюционную. При таком сценарии, всеобщий интерес начинают вызывать устройства, которые смогли бы обеспечить тесное взаимодействие этих технологий не только на физическом уровне, но и на уровнях формирования и предоставления услуг.

Мультисервисная сеть следующего поколения - вот то, чем заняты во всем мире мысли специалистов в области телекоммуникации. Обычная телефонная связь, сотовая связь, огромные ресурсы сети Интернет, IP-телефония, кабельное телевидение (видео по заказу) - всё это должно быть объединено в единую архитектуру. На начальном же этапе развития мультисервисная сеть, скорее всего, будет представлять собой интеграцию сети с коммутацией каналов и сети с коммутацией пакетов. Задачу объединения интеллектуальной периферии сетей связи независимо от применяемых ими технологий решила компания Lucent Technologies, разработав комплекс аппаратных средств и программного обеспечения под названием Softswitch. С точки зрения пакетных сетей (IP и ATM) – это устройство управления медиашлюзами (Media Gateway Controller) и одновременно контроллер сигнализаций (Signaling Controller). Для осуществления всех этих функций, устройство должно уметь работать с протоколами сигнализаций, построенными по совершенно различной архитектуре, и взаимодействовать с медиашлюзами основанными на различных технологиях. Решение поставленных задач в Softswitch осуществляется отделением функций взаимодействия со специализированными протоколами (оборудованием), от функций обработки и маршрутизации вызовов между аппаратной частью и программным ядром устройства. Все сообщения протоколов сигнализации и управления устройствами приводятся к единому виду, удобному для представления в единой программной модели обработки вызовов. Аппаратная часть Softswitch, отвечающая за взаимодействие с внешними устройствами, называется Сервер устройств (Device Server). Сервер устройств может поддерживать как взаимодействие с медиашлюзами определенного типа (коммутаторами ATM, шлюзами IP-телефонии), так и работу со специализированными протоколами сигнализаций (ОКС №7 (MTP, ISUP-R), SIP). Он может быть выполнен в виде отдельно стоящего оборудования (сервер Sun), или в виде платы для установки в общее шасси. Все сервера

устройств обрабатывают сигнальные сообщения и сообщения управления согласно правилам, необходимым при функционировании связанных с ними протоколов. При этом все функции установления, контроля и разрыва соединений выполняются в отдельном устройстве – Сервере вызовов (Call Server). Именно в данном устройстве происходит принятие решений о маршрутизации вызовов, разрешение адресов, отслеживается политика обработки соединений на основе информации, получаемой от устройств интеллектуальной периферии (например, SPINS). Softswitch (программный коммутатор) не является обязательным элементом при построении сети оператора IP-телефонии, но его использование в архитектуре расширяет возможности оператора по предоставлению услуг. Это объясняется тем, что различные операторы IP-телефонии, взаимодействие с которыми неизбежно, могут использовать и используют оборудование различных производителей.

В принципе, процесс конвергенции сетей (процесс создания мультисервисной сети) уже идет полным ходом, и главная проблема на данный момент заключается, пожалуй, в отсутствии единой системы сигнализации. Единой системы сигнализации пока не создано, а вот устройство, позволяющее обрабатывать и преобразовывать различные протоколы сигнализации, уже есть. Это Softswitch, область применения которого демонстрирует рис.2.2.

2.1.2. Построение сети без использования программного коммутатора

На рисунке 2.1 и 2.2 изображены схемы сетей на основе оборудования Cisco и VocalTec, которые изначально предназначены для предоставления услуг по предоплаченным карточкам IP-телефонии (однако не ограничиваются этими возможностями), при этом доступ пользователей к услуге осуществляется с помощью PIN-кода. Схема сети без использования программного коммутатора показана на рисунке 2.1.

При установлении соединения между шлюзами различных зон, шлюз, принимающий звонок, обеспечивает терминацию звонка, в которую входит:

- авторизация вызывающего шлюза, что необходимо для защиты от несанкционированного использования ресурсов сети
- вызов и установка соединения с абонентом через ТФОП.

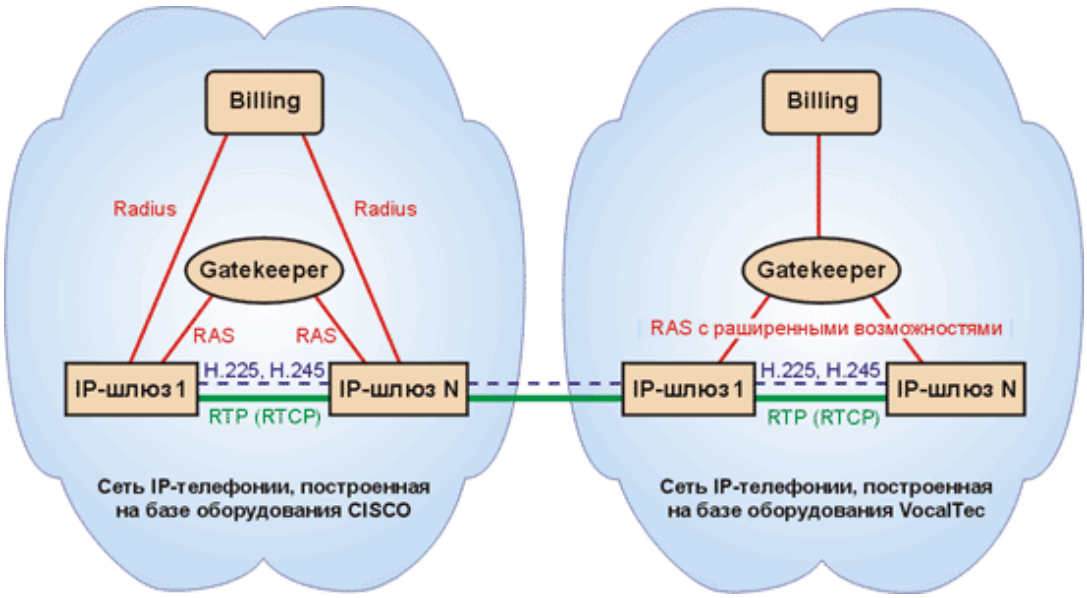


Рис. 2.1. Схема построения и взаимодействия сетей IP-телефонии без использования программного коммутатора

Кроме этого, и вызывающий и терминирующий шлюз осуществляют преобразование речевой и факсимильной информации в вид, пригодный для передачи по IP-сетям, ограничивают время соединения, если клиент израсходовал оплаченное время, и информируют систему биллинга о продолжительности соединения.

Рассмотренные выше схемы имеют следующие недостатки:

- При разрыве связи между шлюзом и сервером биллинга или между шлюзом и контроллером зоны информация о соединении может теряться. Если вызывающий и терминирующий шлюзы принадлежат одной сети, то эту информацию можно восстановить. Если же для

терминации используется шлюз другой сети, то при взаиморасчетах операторов возникает спорная ситуация, когда один оператор простит оплатить его услуги на основании данных своего биллинга, а другой оператор не имеет данных об этих услугах.

- Для защиты от несанкционированного использования своей сети операторы авторизуют шлюзы своих партнеров по IP-адресу. При изменении конфигурации сети одного оператора все его партнеры должны произвести адекватные изменения в настройках своих сетей. Это трудоемкая операция, и не всегда её удается выполнить оперативно и в короткие сроки. Этого недостатка можно было бы избежать, если бы контроллер зоны поддерживал функцию проксирования трафика (когда пакеты с данными от одного шлюза попадают сначала к контроллеру зоны, а затем они переправляются по назначению, к другому шлюзу), тогда при взаимодействии с другими операторами всегда использовался бы только один IP-адрес.
- Протокол H.323 получил неодинаковую трактовку при реализации в оборудовании различных производителей, что затрудняет, а иногда делает невозможной совместную работу сетей, построенных на таком оборудовании.
- Недорогие шлюзы не поддерживают стык с биллингом и не поддерживают нестандартные возможности протокола H.323, которые позволяют стыковать биллинг с контроллером зоны.

2.1.3. Построение сети с использованием программного коммутатора

Если связать шлюзы не напрямую, а через промежуточное устройство - программный коммутатор, к которому подключена система биллинга, то это позволит с минимальными затратами, без кардинального изменения схемы построения существующих сетей избавиться от типичных недостатков традиционных схем IP-телефонии.

Softswitch полностью контролирует ход соединения. При потере связи с одним из шлюзов соединение с другим шлюзом корректно завершается, система учета фиксирует реальное время соединения. Взаимодействие со шлюзами других операторов осуществляется с одного IP-адреса (для них Softswitch выглядит как обычный шлюз). Softswitch корректно взаимодействует со шлюзами различных производителей. И еще одна особенность состоит в том, что он позволяет вести учет соединений с корпоративных шлюзов. Схема сети с использованием программного коммутатора показана на рисунке 2.2.

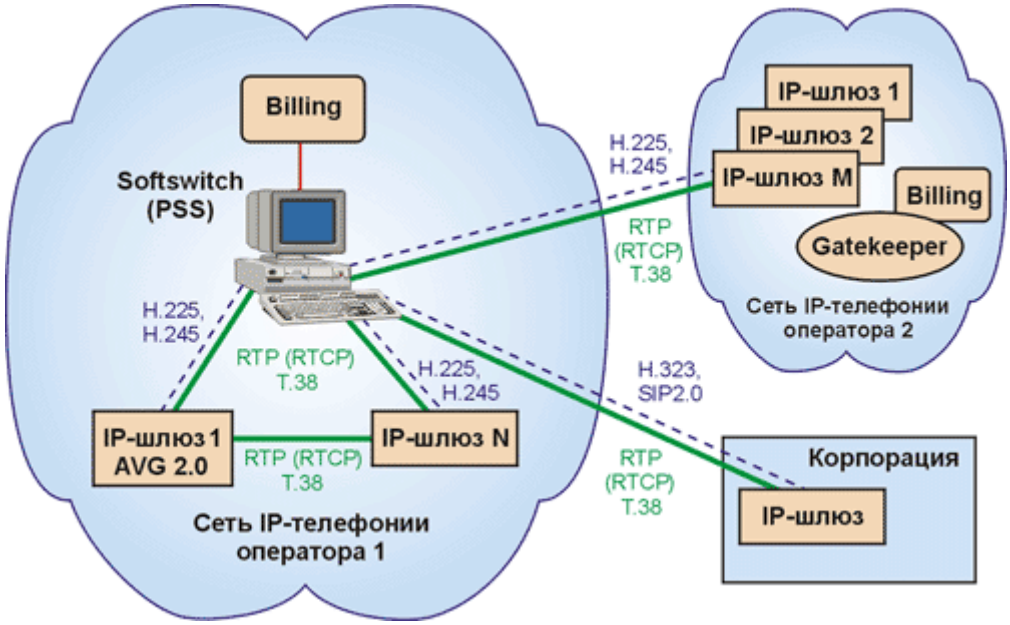


Рис. 2.2. Схема построения и взаимодействия сетей IP-телефонии с использованием программного коммутатора

Кроме того, Softswitch позволяет скрыть структуру сети IP-телефонии при межоператорском взаимодействии, а также подключать в сеть оборудование с сигнализацией отличной от H.323, например, SIP. На рис. 2.2. приведен пример построения сети IP-телефонии с использованием Softswitch (PSS) (в принципе может быть также реализован вариант, когда PSS используется в качестве вспомогательного устройства, т.е. используется как некий

маршрутизатор на границе сетей операторов, в то время как функции привратника и контроля за биллингом отделены и выполняются другими устройствами).

Резюмируя вышесказанное, можно сказать, что наличие программного коммутатора является неотъемлемой частью сети конкурентноспособного оператора IP-телефонии. Его роль возрастает еще больше, если учесть, что при появлении новых видов услуг, разработка современных протоколов делает неизбежным изменение архитектуры построения IP-телефонных сетей.

2.2 Анализ возможностей протоколов IP-телефонии с точки зрения безопасности функционирования сети

2.2.1 Обеспечение безопасности в системах на базе стандарта H.323

Для систем IP-телефонии, построенных на базе Рекомендации ITU-T H.323, вопросы безопасности рассматриваются в Рекомендации H.235. Эта рекомендация описывает ряд технических требований, включая вопросы безопасности: аутентификация пользователей и шифрование данных. Предложенная схема обеспечения безопасности применима и к простым двухточечным и к многоточечным конференциям для любых терминалов, которые используют протокол управления H.245. Если для IP-телефонии стандарта H.323 используются сети с пакетной коммутацией, не обеспечивающие гарантированного качества обслуживания QoS, то по тем же самым техническим причинам не обеспечивается и безопасное обслуживание. Для обеспечения гарантированной связи в реальном масштабе времени по опасным сетям необходимо рассматривать две главных области обеспечения безопасности – аутентификация и секретность. Или, если смотреть более широко, это проблема доступа к сетевым ресурсам и проблема доступности информации непосредственно в каналах мультисервисной сети. Причем проблема доступа к ресурсам сети не ограничивается только аутентификацией пользователя, в результате которой он фактически лишь получает

определенные услуги; речь идет также о доступе к администрированию сети и сетевого оборудования, к базам данных (что очень актуально для компаний, предоставляющих услуги Интернета]

В том числе стоит еще оговорить и возможные проблемы, возникающих в рамках безопасности, при обмене сообщениями аутентификации сетевого оборудования между собой (как то, например, между сетевыми экранами и шлюзом и так далее).

Что же касается проблемы доступности информации непосредственно в каналах сети IP-телефонии, то тут несомненную опасность представляет угроза подслушивания, кратко описанная в первой главе в разделе типы угроз в сетях IP-телефонии.

В соответствии с Рекомендацией H.235 в системе должны быть реализованы четыре основные функции безопасности:

- Аутентификация;
- Целостность данных;
- Секретность;
- Проверка отсутствия долгов.

Аутентификация пользователя обеспечивается управлением доступа в конечной точке сети и выполняется привратником, являющимся администратором зоны H.323. аутентификация основывается на использовании общих ключей с цифровым сертификатом. Для авторизации сертификатов они включают, например, идентификаторы провайдера услуг. Рекомендация H.235 не определяет содержание цифровых сертификатов, используемых соответствующим протоколом аутентификации, а также их генерацию, администрирование и распределение.

Целостность данных и секретность обеспечивается криптографической защитой. Проверка отсутствия долгов гарантируется тем, что конечная точка может отказать в обслуживании вызова. Для обеспечения безопасности

согласно рекомендации H.235 могут использоваться существующие стандарты: IP-безопасность (IP Security – IPSec) и безопасность транспортного уровня (Transport Layer Security – TLS).

Для обеспечения безопасной связи в системе на базе Рекомендации H.323 используются механизмы защиты информации канала управления вызовом Q.931, информации канала управления для мультимедиа коммуникаций H.245, информации каналов передачи мультимедиа. Канал управления вызовом (H.225.0) и канал сигнализации (H.245) должны оба работать в защищенном или незащищенных режимах, начинающимся с первой станции. Для канала управления вызовом защита сделана априорно (для систем в соответствии с Рекомендацией H.323 безопасность транспортного уровня обеспечивается соответствующим протоколом TSAP [порт 1300], который должен использоваться для Q.931 сообщений). Для канала сигнализации режим «защита» определяется информацией, переданной с помощью протокола начальной установки и подключения терминалов стандарта H.323.

2.2.2. Механизмы безопасности в проекте TIPHON

Работа над проектом TIPHON (Telecommunication and Internet Protocol Harmonization over Networks) была начата институтом ETSI в 1997г. Основная задача проекта – решение проблем взаимодействия между сетями с маршрутизацией пакетов IP и сетями с коммутацией каналов в части поддержки прозрачной передачи речевой и факсимильной информации. Под сетями с коммутацией каналов далее будем понимать сети ТФОП, ISDN и GSM.

Основной недостаток архитектуры сети на базе стандарта H.323 заключается в сложности разработки и использования систем IP-телефонии. Охватывая несколько уровней модели OSI, H.323 структурно является довольно сложной рекомендацией, а некоторые ее места допускают неоднозначную трактовку. Так функции безопасности (согласно рекомендации

H.235) определены в H.323 версии 2 как необязательные. Наличие механизмов аутентификации, шифрования и обеспечения целостности информации не исключается, но и не является необходимым условием того, чтобы считать продукт соответствующим H.323.

Упростить процесс внедрения технологии IP-телефонии призван проект TIPHON, реализация которого позволит успешно решить задачи установления, модификации и завершения телефонных соединений, включая процессы межсетевого взаимодействия, управления безопасностью вызова, запроса качества обслуживания, шифрования, аутентификации и другие.

В рамках дипломной работы нас будет в дальнейшем интересовать направление деятельности рабочей группы TIPHON, касающееся аспектов защиты и безопасности. К ним относится первичная защита сети от случайных или умышленных повреждений, защита информации и доступа, аутентификация и авторизация, шифрование данных.

В проект включены следующие механизмы защиты для обеспечения безопасности телефонной связи с конечных устройств, основанные на приложении J рекомендации ITU-T H.323:

- Механизм защиты, основанный на цифровых сертификатах (CBSP);
- Механизм защиты, основанный на паролях (PBSP);
- Механизм защиты, основанный на шифровании информации.

Основным механизмом защиты является использование цифровых сертификатов. Реализация функций безопасности в данном механизме показана в табл.2.1.

В тех странах, где технология CBSP не реализована, должен использоваться механизм на базе паролей. Однако, следует отметить, что PBSP является самым простым механизмом и не обеспечивает уровень защиты, реализуемый при использовании CBSP.

Табл.2.1

Механизм безопасности TIPHON, основанный на сертификатах

Функции безопасности	Функции обслуживания вызовов		
	RAS	H.225.0	H.245
Аутентификация	Цифровая подпись SHA1/MD5 (Процедура A)	Цифровая подпись SHA1/MD5 (Процедура A)	Цифровая подпись SHA1/MD5 (Процедура A)
Отказ при наличии долгов	Цифровая подпись SHA1/MD5 (Процедура A)	Цифровая подпись SHA1/MD5 (Процедура A)	Цифровая подпись SHA1/MD5 (Процедура A)
Целостность информации	Цифровая подпись SHA1/MD5 (Процедура A)	Цифровая подпись SHA1/MD5 (Процедура A)	Цифровая подпись SHA1/MD5 (Процедура A)
Управление ключами	Распределение сертификата	Распределение сертификата и обмен ключами для аутентификации по алгоритму Даффи-Хофмана	Управление общим ключом сеанса связи H.235 (распределение ключа, изменение ключа)

Криптографическая защита информации является необязательным требованием и используется только в сценариях, когда необходимо обеспечить секретность передаваемой информации. Оба механизма CBSP и PBSP используют модель безопасности при маршрутизации через шлюз на базе Приложения F Рекомендации H.323.

2.2.3. Обеспечение безопасности на базе протокола OSP

Компании 3Com, Cisco и ряд других сообщили о поддержке предварительного стандарта IP-телефонии – Open Settlement Protocol (OSP), - который предназначен для решения взаимодействия сетей различных

провайдеров. Это простой протокол, позволяющий различным компаниям – владельцам средств связи осуществлять коммуникации в пределах всей страны. К примеру, он позволяет устанавливать автора звонка, санкционировать обслуживание вызова и указывать расчетную информацию, которая будет включена в записи, содержащие подробные данные об этой транзакции.

Рабочая группа института ETSI одобрила этот протокол, а производители в ближайшее время намерены провести его тестирование. Новый протокол был разработан в рамках проекта TIPHON. Протоколу OSP еще предстоит пройти процедуру окончательной ратификации. Однако ведущие компании, предоставляющие услуги IP-телефонии, включая Ascend, GTE, AT&T и Internet Telephony Exchange Carrier (ITXC), уже заявили о поддержке протокола OSP. В то же время компании Lucent и Nortel выразили свою заинтересованность и в целом готовы поддержать стандарты на IP-телефонию, но от окончательной оценки OSP пока воздержались.

Основные характеристики спецификации Open Settlement Protocol (OSP):

- Шифрование Secure Sockets Layer;
- Безопасная аутентификация участников сеанса связи с помощью шифрования открытым и частным ключами;
- Поддержка технологии цифровой подписи;
- Обмен информации с помощью XML.

При условии внедрения единого способа выполнения аутентификации и обеспечения взаимосвязи различных сетей значительно упростится задача выбора провайдера услуг IP-телефонии. В настоящее время ни один провайдер не может пока предлагать свои услуги во всех регионах, а стандартный подход позволит им обеспечить более «прозрачные» службы и в более широкой географической области. Однако при этом возникает целый ряд вопросов. В частности, пока не установлено, каким образом сети будут взаимодействовать

друг с другом на уровне расчетов. Кроме того, расширение географии расширит и потенциальные возможности злоумышленников, а следовательно стоит серьезно отнестись к обозначенным механизмам обеспечения безопасности.

2.2.4 Вопросы безопасности в протоколах SIP и MGCP

Данный протокол, похожий на HTTP и используемый абонентскими пунктами для установления соединения не обладает серьезной защитой и ориентирован на применение решений третьих фирм (например, PGP). В качестве механизма аутентификации RFC 2543 предлагает несколько вариантов и, в частности, базовую аутентификацию (как в HTTP) и аутентификацию на базе PGP. Пытаясь устранить слабую защищенность данного протокола, Майкл Томас из компании Cisco Systems разработал проект стандарта IETF, названный "SIP security framework", который описывает внешние и внутренние угрозы для протокола SIP и способы защиты от них. В частности, к таким способам можно отнести защиту на транспортном уровне с помощью TLS или IPSec. Компания Cisco в своей архитектуре безопасности корпоративных сетей SAFE, очень большое внимание уделяет практическим вопросам защиты IP-телефонии.

Стандарт MGCP, определенный в RFC 2705 и неприменяемый на оконечных устройствах (шлюзы MGCP могут работать как с компонентами, поддерживающими H.323, так и с компонентами, поддерживающими SIP), использует для защиты голосовых данных протокол ESP спецификации IPSec. Может также использоваться и протокол AH (но только не в сетях IPv6), который обеспечивает аутентификацию и целостность данных (connectionless integrity) и защиту от повторений, передаваемых между шлюзами. В то же время, протокол AH не обеспечивает конфиденциальности данных, которая достигается применением ESP (наряду с другими тремя защитными функциями).

3. Обеспечение безопасности с точки зрения проверки прав доступа к ресурсам (AAA)

Сеть IP-телефонии любого провайдера, как правило, имеет несколько точек доступа к услуге; при такой схеме организации реализовывать процесс аутентификации пользователей для каждой точки доступа в отдельности (на месте) не целесообразно. Гораздо разумнее ценрализовать процесс аутентификации, используя для этого отдельный сервер и общую базу данных, к которым будут обращаться серверы доступа (такое решение получило название непрямой аутентификации). Объясняется это главным образом с точки зрения проблем администрирования, возникающих в случае организации аутентификации на месте.

3.1. Непрямая аутентификация

Непрямая аутентификация – модель, в которой механизм аутентификации размещается в стороне от других серверов сети, при этом они связываются с ним каждый раз, когда пользователь запрашивает доступ.

Решения на основе непрямой аутентификации позволяют справляться с проблемой масштабируемости на вычислительных центрах, у которых одна группа пользователей, но несколько точек обслуживания. Даже на той площадке, где всего два сервера, будет затруднительно поддерживать совместимость двух отдельных баз данных аутентификации. Если другие проектные шаблоны предусматривают объединение механизмов аутентификации и управления доступом, то шаблон непрямой аутентификации перемещает механизм аутентификации из точки обслуживания в отдельный аутентификационный сервер. Все другие компоненты сети предоставляют услуги или управляют доступом к ресурсам, но не принимают решений об аутентификации. Вместо этого они аутентифицируют пользователей

непрямым способом, связываясь с аутентификационным сервером всякий раз, когда кто-то пытается зарегистрироваться в системе.

Как уже отмечалось во второй главе с точки зрения обеспечения безопасности соединения как в сетях IP-телефонии в частности, так и в IP-сетях вообще, проблему можно условно разделить на две составляющих. Первое – это проблема обеспечения правомерного и безопасного доступа к сетевым ресурсам и услугам, а второе – это обеспечение безопасности информации уже непосредственно в каналах. Именно первой части проблемы обеспечения безопасности в сетях IP-телефонии и посвящена эта глава.

Совершенно очевидно, что основная роль при решении подобных задач будет принадлежать процессу аутентификации пользователей. В силу структуры мультисервисной сети, на базе которой предоставляются услуги IP-телефонии (см. главу 2 дипломной работы) нас будет интересовать непрямая аутентификация, ее протоколы, а также слабые и сильные места.

Многие широко известные сегодня системы обеспечивают непрямую аутентификацию с помощью специально разработанных протоколов. Открытым стандартом для реализации непрямой аутентификации является протокол RADIUS. В общем случае протокол непрямой аутентификации начинает свою работу, когда кто-нибудь пытается зарегистрироваться в точке обслуживания с удаленного места, которым может быть, например, рабочая станция. Когда точка обслуживания принимает запрос на регистрацию, она пересылает имя пользователя и пароль аутентификационному серверу. Часто для пересылки данных таких сообщений используется внутренний протокол типа RADIUS или протокол, разработанный изготовителем. Если сервер подтверждает аутентификацию, то он посылает в точку обслуживания подтверждение, сформатированное в соответствии с этим внутренним протоколом. Получив его, точка обслуживания принимает к исполнению попытку пользователя зарегистрироваться. Если сервер посылает отказ, то точка обслуживания отвергает запрос. Поскольку аутентификационные

запросы перенаправляются аутентификационному серверу, имеется риск, что взломщик будет подделывать сообщение «Доступ разрешен», чтобы обмануть точку доступа; поэтому для аутентификации двусторонних сообщений между точкой обслуживания и аутентификационным сервером должно использоваться шифрование.

Некоторые системы, использующие непрямую аутентификацию, могут иметь высокий уровень устойчивости к отказам, поддерживая функцию перенаправления. Если какой-либо из серверов теряет работоспособность (в том числе и при DOS-атаке), то запросы на аутентификацию могут перенаправляться на альтернативный сервер, содержащий копию всей аутентификационной базы данных. Это позволяет провайдеру IP-телефонии реплицировать свои службы на несколько хост-машин и реализовать аутентификацию на нескольких аутентификационных серверах, исключая тем самым появление точки критического отказа.

Например, сетевой оборудование компании Cisco Sistems поддерживает три протокола сервера защиты – TACACS+, RADIUS и Kerberos. Первые два являются на сегодня главными протоколами сервера защиты, используемыми для решения задач AAA с серверами сетевого доступа, шлюзами IP-телефонии, маршрутизаторами и брандмауэрами.

3.2. Технологии AAA на основе протокола TACACS+

3.2.1. Протокол TACACS+

TACACS – это простой протокол управления доступом, основанный на стандартах UDP и разработанных компанией Bolt, Beranek and Newman, Inc. (BBN). Компания Cisco несколько раз совершенствовала и расширяла протокол TACACS, и в результате появилась ее собственная версия, известная как TACACS+.

TACACS+ представляет собой приложение сервера защиты, позволяющее на основе соответствующего протокола реализовать централизованное управление доступом пользователей к услугам. Информация о сервисах TACACS+ и пользователях хранится в базе данных, обычно размещенной на компьютере под управлением UNIX или Windows NT. TACACS+ позволяет с помощью одного сервера управления приложениями реализовать независимую поддержку сервисов AAA.

Протокол TACACS+ работает по технологии клиент-сервер. Фундаментальным структурным компонентом протокола TACACS+ является разделение аутентификации, авторизации и учета. Это позволяет обмениваться идентификационными сообщениями любой длины и содержания, и, следовательно, использовать для клиентов TACACS+ любой идентификационный механизм, в том числе PPP PAP, PPP CHAP, аппаратные карты и т.д.

3.2.2. Свойства протокола TACACS+

TACACS+ поддерживает следующие возможности сервера защиты:

- *Пакеты TCP для надежной передачи данных*. Использование TCP в качестве протокола связи для соединений TACACS+ между сервером доступа и сервером защиты. Для TACACS+ резервируется TCP-порт 49.
- *Архитектура AAA*. Каждый сервис предоставляется отдельно и имеет собственную базу данных, но, тем не менее, они работают вместе, как один сервер защиты.
- *Канальное шифрование.* Часть TCP-пакета, содержащая данные протокола TACACS+, шифруется с целью защиты трафика между сервером доступа и сервером защиты.
- *Каждый пакет TACACS+ имеет 12-байтовый заголовок, пересылаемый в виде открытого текста, и тело переменной длины, содержащее*

параметры TACACS+. Тело пакета шифруется с помощью алгоритма, использующего псевдослучайный заполнитель, получаемый посредством MD5. Пакеты TACACS+ передаются по сети и хранятся сервером TACACS+ в шифрованном виде. Когда это необходимо, пакет дешифруется сервером доступа и приложением TACACS+ путем обращения алгоритма шифрования.

- *Аутентификация PAP и CHAP*. Обеспечивает полный контроль аутентификации с помощью средств вызова/ответа PAP и CHAP, а также посредством использования диалоговых окон ввода пароля доступа и поддержки сообщений интерактивной процедуры начала сеанса.
- *Защита локальных и глобальных сетей*. Поддержка средств AAA удаленного и локального сетевого доступа для серверов доступа, маршрутизаторов и другого сетевого оборудования, поддерживающего TACACS+. Дает возможность осуществлять централизованное управление сетевым оборудованием.
- *Функция обратного вызова*. Данная функция возвращает телефонные вызовы, заставляя сервер доступа звонить соответствующему пользователю, что может дать дополнительные гарантии защиты.
- *Индивидуальные списки доступа пользователей*. База данных TACACS+ может дать указание серверу сетевого доступа контролировать доступ данного пользователя к сетевым службам и ресурсам в течении фазы авторизации на основе списка доступа.

3.2.3. Процессы AAA в протоколе TACACS+

Аутентификация не является обязательной. Она рассматривается как опция, которая конфигурируется на месте. В некоторых местах она вообще не требуется, в других местах она может применяться лишь для ограниченного набора услуг.

Заголовок пакета TACACS+ содержит поле типа, являющееся признаком того, что пакет представляет собой часть процесса AAA. Аутентификация TACACS+ различает три типа пакетов: START (начало), CONTINUE (продолжение) и REPLY (ответ).

В запросе на авторизацию можно указать, что аутентификация пользователя не проведена (личность не доказана). В этом случае лицо, отвечающее за авторизацию должно самостоятельно решить, допускать такого пользователя к запрашиваемым услугам или нет. Протокол TACACS+ допускает только положительную или отрицательную авторизацию, однако этот результат допускает настройку на потребности конкретного заказчика. Авторизация может проводиться на разных этапах, например, когда пользователь впервые входит в сеть и хочет открыть графический интерфейс или когда пользователь запускает PPP и пытается использовать поверх PPP протокол IP с конкретным адресом IP. В этих случаях демон сервера TACACS+ может разрешить предоставление услуг, но наложить ограничения по времени или потребовать список доступа IP для канала PPP.

В процессе авторизации TACACS+ используется два типа пакетов: REQUEST (запрос) и RESPONSE (ответ). Данный процесс авторизации пользователя контролируется посредством обмена парами «атрибут/значение» между сервером защиты TACACS+ и сервером доступа.

Аудит (или учет) обычно следует за аутентификацией и авторизацией. Учет представляет собой запись действий пользователя. В системе TACACS+ учет может выполнять две задачи. Во-первых, он может использоваться для учета использованных услуг (например, для выставления счетов). Во-вторых, его можно использовать в целях безопасности. Для этого TACACS+ поддерживает три типа учетных записей. Записи «старт» указывают, что услуга должна быть запущена. Записи «стоп» говорят о том, что услуга только что окончилась. Записи «обновление» (update) являются промежуточными и указывают на то, что услуга все еще предоставляется. Учетные записи TACACS+ содержат всю

информацию, которая используется в ходе авторизации, а также другие данные: время начала и окончания (если это необходимо) и данные об использовании ресурсов. Транзакции между клиентом TACACS+ и сервером TACACS+ идентифицируются с помощью общего «секрета», который никогда не передается по каналам связи. Обычно этот «секрет» вручную устанавливается на сервере и на клиенте. TACACS+ можно настроить на шифрование всего трафика, который передается между клиентом и демоном сервера TACACS+.

В процессе аудита TACACS+ использует два типа пакетов – REQUEST (запрос) и RESPONSE (ответ). Данный процесс во многом подобен процессу авторизации. В процессе аудита создаются записи с информацией об активности пользователя в отношении заданных сервисов. Записи, регистрирующие выполненные сетевым оборудованием действия, могут сохраняться в некотором стандартном формате, на сервере защиты с целью дальнейшего анализа.

В рамках TACACS+ аудит AAA не является средством надежной защиты и обычно используется только для учета или управления. Однако с помощью аудита AAA можно контролировать действия пользователя, чтобы, например, вовремя заметить его необычное поведение при работе с сетевым оборудованием.

3.3. Технологии AAA на базе протокола RADIUS

3.3.1. Протокол RADIUS

Протокол RADIUS был разработан компанией Livingston Enterprises, Inc. (теперь находящейся в составе Lucent Technologies) в качестве протокола аутентификации серверного доступа и учета. В настоящее время протокол RADIUS описывается в документе RFC 2865, а аудит RADIUS – в RFC 2866.

RADIUS (Remote Access Dial-In User Service – сервис идентификации удаленных абонентов) представляет собой распределенный протокол,

используемый в рамках технологии клиент/сервер и обеспечивающий защиту сети от несанкционированного доступа. Так например компания Cisco поддерживает RADIUS как одну из составляющих системы защиты AAA. Рассматриваемый протокол скорее объединяет аутентификацию и авторизацию, чем трактует их отдельно, как это делается в отношении аудита. Протокол RADIUS может использоваться с другими протоколами защиты AAA, например с TACACS+, Kerberos и локальными базами данных защиты.

Протокол RADIUS реализован во многих сетевых средах, требующих высокого уровня защиты при условии поддержки сетевого доступа для удаленных пользователей. Он представляет собой полностью открытый протокол, поставляемый в формате исходного текста, который можно изменить для того, чтобы он мог работать с любой доступной в настоящий момент системой защиты. Широкую популярность RADIUS обеспечивает возможность добавлять новые пары «атрибут/значение» в дополнение к тем, которые описаны в документе RFC 2865. Протокол RADIUS имеет атрибут поставщика (атрибут 26), позволяющий поставщику осуществлять поддержку своих собственных расширенных наборов атрибутов, включающих нестандартные атрибуты. Вследствие использования пар «атрибут/значение» конкретных поставщиков могут возникать трудности при интеграции серверных продуктов защиты RADIUS в другие системы защиты. Серверы защиты RADIUS и соответствующие клиенты должны игнорировать нестандартные пары «атрибут/значение», созданные конкретными поставщиками.

Связь между NAS и сервером RADIUS основана на протоколе UDP. В целом считается, что протокол RADIUS не имеет отношения к подключению. Все вопросы, связанные с доступностью сервера, повторной передачей данных и отключениями по истечении времени ожидания, контролируются устройствами, работающими под управлением протокола RADIUS, но не самим протоколом передачи. Протокол RADIUS основан на технологии

клиент-сервер. Клиентом RADIUS обычно является NAS, а сервером RADIUS считается «демон», работающий на машине UNIX или NT. Клиент передает пользовательскую информацию на определенные серверы RADIUS, а затем действует в соответствии с полученными от сервера инструкциями. Серверы RADIUS принимают запросы пользователей на подключение, проводят идентификацию пользователей, а затем отправляют всю конфигурационную информацию, которая необходима клиенту для обслуживания пользователя. Для других серверов RADIUS или идентификационных серверов других типов сервер RADIUS может выступать в роли клинта-посредника (proxy).

3.3.2. Свойства и возможности протокола RADIUS

RADIUS поддерживает следующие возможности сервера защиты:

- *Пакеты UDP*. Для связи RADIUS между сервером доступа и сервером защиты используется протокол UDP и UDP-порт 1812, официально назначенный для этого. Некоторые реализации RADIUS используют UDP-порт 1645. Использование UDP упрощает реализацию клиента и сервера RADIUS.
- *Объединение аутентификации и авторизации и выделение аудита.* Сервер RADIUS получает запросы пользователя, выполняет аутентификацию и обеспечивает клиенту информацию о конфигурации. Аудит выполняется сервером аудита RADIUS.
- *Шифрование паролей пользователей.* Пароли, содержащиеся в пакетах RADIUS (а это только пользовательские пароли), шифруются посредством хэширования MD5.
- *Аутентификация PAP и CHAP*. Обеспечивает управление аутентификацией с помощью средств вызова/ответа PAP и CHAP, а также посредством диалога начала сеанса и ввода пароля наподобие входа в систему UNIX.

- *Защита глобальной сети.* Обеспечивает поддержку средств AAA удаленного доступа для серверов доступа многих поставщиков, поддерживающих клиентов RADIUS. Дает возможность централизовать управление удаленным доступом.
- *Поддержка ряда протоколов, обеспечивающих терминальный доступ к серверу защиты RADIUS.*
- *Функция обратного вызова.* Данная функция возвращает телефонные вызовы, заставляя сервер доступа звонить соответствующему пользователю, что может дать дополнительные гарантии защиты пользователям, использующим доступ по телефонным линиям.
- *Расширяемость.* Все транзакции предполагают использование пар «атрибут/значение» переменной длины. Новые атрибуты могут быть добавлены в существующие реализации протокола.
- *Гарантированная сетевая защита.* Аутентификация транзакций между клиентом и сервером защиты RADIUS предполагает использование общего секретного значения.

3.3.3. Процесс аутентификации и авторизации в протоколе RADIUS

Клиент RADIUS и сервер защиты RADIUS обмениваются пакетами Access-Request (доступ-запрос), Access-Accept (доступ-подтверждение), Access-Reject (доступ-отказ) и Access-Challenge (доступ-вызов). Как показано на рис. 3.1, при попытке подключиться к серверу сетевого доступа, имеющему конфигурацию клиента RADIUS, выполняются следующие шаги:

- Пользователь инициализирует запрос аутентификации PPP к серверу сетевого доступа.
- У пользователя запрашивается имя пользователя и пароль
- Сервер сетевого доступа посылает серверу защиты RADIUS пакет Access-Request, содержащий имя пользователя, шифрованный пароль и другие атрибуты.

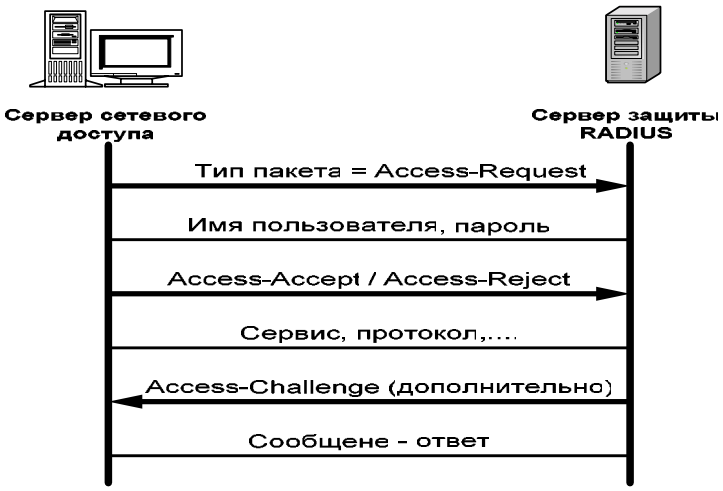


Рис.3.1. Процесс аутентификации и авторизации RADIUS

- Сервер защиты RADIUS идентифицирует клиента-инициатора, выполняет аутентификацию пользователя, проверяет параматры авторизации пользователя и возвращает один из следующих ответов:

  Access-Accept – пользователь аутентифицирован.

  Access-Reject – пользователь не аутентифицирован, и сервер сетевого доступа либо предлагает ввести имя пользователя и пароль снова, либо запрещает доступ.

  Access-Challenge – вызов является дополнительной возможностью сервера защиты RADIUS.
- Сервер сетевого доступа обращается к параметрам аутентификации, разрешающим использование конкретных служб.
- Ответ Access-Accept или Access-Reject связывается с дополнительными данными (парами «атрибут/значение»), используемыми для сеансов EXEC и авторизации. Процесс аутентификации RADIUS должен быть завершен до начала процесса авторизации.
- Сервер защиты RADIUS может периодически посылать пакеты Access-Challenge серверу сетевого доступа, чтобы потребовать повторного введения имени пользователя и пароля пользователем, информировать о состоянии сервера сетевого доступа или выполнить какие-то другие

действия, предусмотренные разработчиками сервера RADIUS. Клиент RADIUS не может посылать пакеты Access-Challenge.

3.3.4. Процесс аудита на базе протокола RADIUS

Протокол RADIUS был усовершенствован с тем, чтобы обеспечить доставку информации аудита от клиента RADIUS серверу аудита RADIUS через UDP-порт 1813. Клиент RADIUS отвечает за отправку информации аудита пользователя соответствующему серверу аудита RADIUS, для чего используется пакет типа Accounting-Request (аудит-запрос) с соответствующим набором пар «атрибут/значение». Сервер аудита RADIUS должен принять запрос аудита и вернуть ответ, подтверждающий успешное получение запроса. Для этого используется пакет типа Accounting-Response (аудит-ответ).

Как видно из рис. 3.2, при попытке подключиться к серверу сетевого доступа, имеющему конфигурацию клиента RADIUS, выполняются следующие шаги:

1. После исходной аутентификации сервер сетевого доступа посылает серверу защиты RADIUS старт-пакет Accounting-Request.
2. Сервер защиты RADIUS подтверждает получение старт-пакета, возвращая пакет Accounting-Response.
3. По окончании использования сервиса сервер сетевого доступа посылает стоп-пакет Accounting-Request; в этом пакете указывается тип предоставленного сервиса и дополнительные статистические данные.
4. Сервер защиты RADIUS подтверждает получение стоп-пакета, возвращая пакет Accounting-Response.

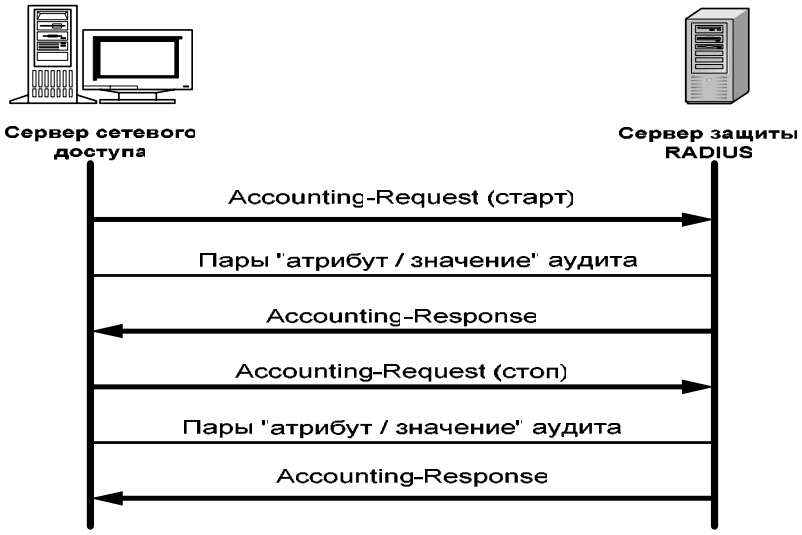


Рис. 3.2. Процесс аудита RADIUS

3.3.5. Сравнение возможностей протоколов TACACS+ и RADIUS

Хотя TACACS+ и RADIUS очень похожи по своим функциональным возможностям, они имеют несколько важных отличий, указанных в табл.3.1.

Табл.3.1.

Сравнение протоколов TACACS+ и RADIUS.

Функциональные возможности	TACACS+	RADIUS
Поддержка AAA	Разделение трех сервисов AAA	Аутентификация и авторизация объединяются, а аудит отделяется
Транспортный протокол	TCP	UDP
Обмен сообщениями между клиентом и сервером защиты	Двунаправленный	Однонаправленный
Поддержка протоколов удаленного и межсетевого доступа	Полная поддержка	Отсутствует поддержка NetBEUI
Целостность данных	Шифруется весь пакет TACACS+	Шифруются только пароли пользователей
Возможность перенаправления запроса	Нет	Есть

Помимо этого TACACS+ поддерживает двунаправленный поток вызовов/ответов между серверами сетевого доступа подобно тому, как это сделано в CHAP. RADIUS поддерживает однонаправленный вызов/ответ от сервера защиты RADIUS к клиенту RADIUS.

Целостность данных. TACACS+ предполагает шифрование содержимого пакетов. RADIUS предусматривает шифрование только атрибутов пароля в пакете Access-Request. Это означает лучшую защищенность TACACS+.

Кроме того, сравнивая TACACS+ и RADIUS, можно отметить следующие:

- *Возможности настройки*. Гибкость протокола TACACS+ обеспечивает возможность настройки множества параметров в соответствии с требованиями отдельных пользователей. Из-за недостаточной гибкости RADIUS многие возможности, доступные в рамках TACACS+, при использовании RADIUS недоступны (например, каталоги сообщений). Однако, RADIUS поддерживает возможность изменения наборов пар «атрибут/значение».
- *Процесс авторизации*. При использовании TACACS+ сервер принимает или отвергает запрос аутентификации на основании данных пользовательского профиля. Клиенту (NAS) содержимое пользовательского профиля остается неизвестным. В системе RADIUS все посылаемые с ответом атрибуты пользовательского профиля передаются серверу сетевого доступа. Сервер принимает или отвергает запрос аутентификации на основании полученных им значений атрибутов.

  По большому счету протокол RADIUS не поддерживает авторизацию. То есть RADIUS есть смысл использовать только там, где заранее известно какой сервис предоставляет конкретный RADIUS-клиент. У TACACS+ заложена поддержка авторизации. Но следует отметить, что количество авторизуемых сервисов довольно ограничено в текущей. То есть для доступа к какому-либо сервису

RADIUS обрабатывает один запрос (аутентификацию - запрос, ответ), а TACACS+ - два (аутентификацию и авторизацию), но при этом при использовании TACACS+ есть возможность получить доступ к другому сервису.

- *Аудит*. Аудит TACACS+ предполагает использование ограниченного числа информационных полей. Аудит RADIUS может предоставить больше информации, чем можно получить из записей аудита TACACS+, что является главным преимуществом в сравнении с TACACS+.
- *Возможность перенаправления запроса*. В TACACS+ такая возможность просто отсутствует. RADIUS-протокол же имеет такую возможность. Это очень существенное достоинство этого протокола, в случае если есть представительства оператора IP-телефонии в других регионах. В этом случае клиент, находясь в другом регионе, набирает код доступа (номер и пин-код). Далее местный RADIUS-сервер перенаправляет запрос в соответствующий регион. Происходит аутентификация, и ответ отправляется назад. Таким образом, RADIUS позволяет проектировать гибкую распределенную систему.

RADIUS базируется на протоколе UDP (пакетная передача данных, без гарантии передачи пакета). Следовательно, RADIUS-клиент на любой запрос должен дожидаться ответа от сервера в течение некоторого времени (timeout'a) и в случае отсутствии оного перепослать пакет еще раз. TACACS+ клиент тоже должен дожидаться всегда ответа от сервера, но в отличии от RADIUS-клиента, в случае отсутствия ответа, пакет еще раз не посылается. Гарантия доставки обеспечивается тем, что для обработки какого-либо запроса TACACS+ сервер и клиент должны установить TCP-соединение (даже если весь процесс будет состоять из посылки и приема 2-ух небольших пакетов), а с

точки зрения времени это довольно длительный процесс (по этой причине TACACS+ по определению относительно медленен). На основании этого, можно сказать, что RADIUS будет более эффективен в сетях, где процент потерянных пакетов менее 5-10 %; в других сетях лучше использовать TACACS+. Именно по этой причине в сетях IP-телефонии, где необходимо быстродействие применяется, как правило, протокол RADIUS.

3.3.6. Слабые места процессов AAA с точки зрения несанкционированного доступа в протоколе RADIUS

3.3.6.1. Типы угроз, с которыми должен справляться протокол RADIUS

Рассмотрим более подробно протокол RADIUS. Сегодня, многие провайдеры IP-телефонии отдают предпочтение именно ему (не исключением стали и питерские провайдеры: Петерстар, BCL, Comset и т.д.). Это происходит отчасти по причинам, о которых говорилось в главе 1. Вместе с тем, с точки зрения безопасности протокол RADIUS, на первый взгляд, уступает протоколу TACACS+ . Именно поэтому, наверно, имеет смысл поговорить о возможных проблемах, связанных с использованием этого протокола, и о его уязвимых местах.

Протокол RADIUS укладывается в общую картину непрямой аутентификации. В спецификации этого протокола, вообще говоря, вместо термина «клиент» используется термин «агент», так как RADIUS является протоколом для архитектуры клиент-сервер, и агент исполняет роль «клиента». Однако, далее здесь будет использоваться термин агент, чтобы избежать путаницы при определении действий человека, пытающегося зарегистрироваться в системе.

Когда кто-либо пытается войти в систему, агент протокола RADIUS посылает сообщение «Запрос на доступ». Сервер аутентификации отвечает

либо сообщением «Доступ разрешен», либо «В доступе отказано». Однако, в протоколе RADIUS есть несколько дополнительных битов усложнения, которые защищают агента и сервер от атак. Существует достаточно способов, с помощью которых атакующая сторона может воспользоваться или вмешаться в аутентификационные сообщения, посылаемые клиентской рабочей станцией. Эти атаки служат пределами области действия протокола RADIUS, поскольку он описывает сообщения между агентом и севером. Однако, многие из атак на сообщения между клиентом и агентом могут также представлять угрозу и для сообщений между агентом и сервером аутентификации.

Рассмотрим следующий пример: команда злоумышленников из двух человек пытается получить доступ к сетевым ресурсам. Злоумышленник 1 находится вне организации и пытается войти в систему. Злоумышленник 2 подключается к системе внутри организации и использует свое положение, чтобы помочь первому выдать себя за авторизованного пользователя. Какие атаки могут быть предприняты?

- Для начала, злоумышленник 2 может разместиться между агентом и сервером аутентификации. Когда злоумышленник 1 попытается зарегистрироваться, второй может перехватить запрос на аутентификацию к серверу и послать поддельный аутентификационный ответ, который верифицирует попытку злоумышленника 1 войти в систему. Если агент не сможет распознать подделку, то он будет успешно зарегистрирован.
- Существует несколько способов защиты от атак подделки статуса. Но даже если протокол включает в себя такую защиту, могут быть и другие пути достижения того же результата. Например, злоумышленник 2 может перехватить пакеты в пути их следования между сервером и агентом, модифицировать их на лету и послать дальше по назначению. В частности, он может перехватить

сообщение «В доступе отказано», посланное в ответ на сообщение первого злоумышленника «Запрос на доступ», и преобразовать его в сообщение «Доступ разрешен». Сделать это можно, изменив в сообщении «В доступе отказано» всего один бит.

- Даже если протокол имеет защиту от подделок и модификаций, все равно существует еще одна опасность. Так злоумышленник 2 может перехватить законные сообщения, курсирующие между агентом и сервером, и попытаться их воспроизвести, чтобы обманным путем заставить агента принять попытку первого злоумышленника войти в систему. Если сервер аутентификации посылает «консервированный» набор ответов на законные запросы о входе в систему, то злоумышленник 2 может просто отобрать нужный ему и послать его агенту. Механизм защиты криптографической целостности не обнаружит воспроизведенное сообщение без наличия дополнительной защиты от воспроизведения.

Итак, имеется три основных типа атак, с которыми должен уметь справляться протокол RADIUS:

- воспроизведение сообщений, посылаемых в любом из направлений;
- подделка сообщений, особенно тех, что посылаются от сервера агенту;
- модификация сообщений от сервера к агенту.

Возможно, все эти аспекты работы протокола RADIUS выглядят странными, но они начинают приобретать смысл, если рассмотреть, как этот протокол противостоит подобным атакам.

На верхнем уровне протокол RADIUS довольно прост. На рис. 3.3 показано, как он использует одно сообщение, посылаемое от агента серверу, и ответ сервера агенту.

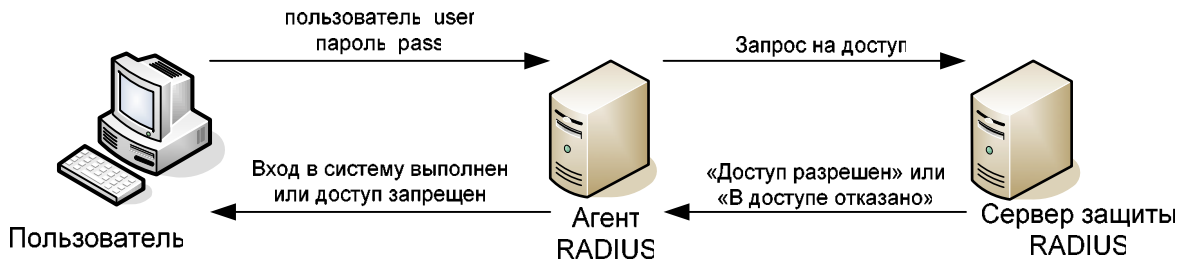


Рис. 3.3. Базовые операции взаимодействия в рамках протокола RADIUS

Когда кто-либо инициирует процедуру регистрации, агент получает имя пользователя и пароль и помещает их в сообщение «Запрос на доступ». В общем случае сообщение содержит следующие данные:

- числовой код, указывающий, что это сообщение типа «Запрос на доступ»;
- восьмибитовый идентификатор для этого запроса на вход;
- длину всего сообщения протокола RADIUS;
- 128-битовое случайное одноразовое число, называемое аутентификатором запроса;
- идентификатор агента, делающего запрос;
- имя пользователя (эти данные необязательны);
- введенный пароль, зашифрованный для передачи;
- необязательные данные типа номера порта, с которого пришел запрос на установление соединения.

После получения этого сообщения сервер аутентификации извлекает из него имя пользователя, дешефрирует пароль и сравнивает информацию с той, что имеется у него в базе данных пользователей. Если пароли совпадают, то сервер посылает агенту сообщение «Доступ разрешен». В общем случае это сообщение содержит следующие данные:

- числовой код, указывающий, что данное сообщение является сообщением типа «Доступ разрешен»;

- восьмибитовый идентификатор, скопированный из сообщения «Запрос на доступ»;
- длину всего сообщения протокола RADIUS;
- хешированное значение, называемое аутентификатором ответа, которое служит для выявления атак;
- необязательную цепочку символов, передаваемых пользователю;
- необязательные данные, описывающие права и полномочия пользователя.

Агент получает это сообщение и анализирует его содержимое с целью проверки на подделку. Затем он использует восьмибитовый идентификатор для соотнесения сообщения с отложенной регистрацией. После этого агент проверяет числовой код сообщения и разрешает регистрацию, если код соответствует сообщению «Доступ разрешен», и отклоняет ее в противном случае.

3.3.6.2. Защита сообщений в протоколе RADIUS

Для надежного использования протокола RADIUS аутентификация выполняется дважды. Сначала надо аутентифицировать сервер, чтобы потом безопасно аутентифицировать пользователя. Когда агент принимает сообщение «Доступ разрешен», он должен быть уверен, что сообщение приходит от сервера, которому он доверяет. Нельзя позволить кому-либо обмануть агента. Более того, весь процесс аутентификации должен быть защищен в возможно большой степени.

Основой аутентификации является базовый секрет. В случае протокола RADIUS секрет – это паролевое слово или паролевая фраза, которая известна серверу и агенту. Секрет используется для шифрования пароля перед его отсылкой, а также для вычисления правильного хеша аутентификатора ответа в сообщении «Доступ разрешен» или «В доступе отказано».

В сообщении «Доступ разрешен» имеется два средства защиты от атак. Первым средством является 128-разрядное случайное число однократного использования, называемое аутентификатором ответа. Агент выбирает новое значение однократно используемого числа случайным образом для каждого запроса на вход в систему, который он обрабатывает. При правильной процедуре выбора шансы на то, что злоумышленник сможет спрогнозировать значение случайного числа чрезвычайно малы. На рис. 3.4 показано, как сервер использует случайное число для построения хешированного значения аутентификатора ответа, которое он посылает агенту.

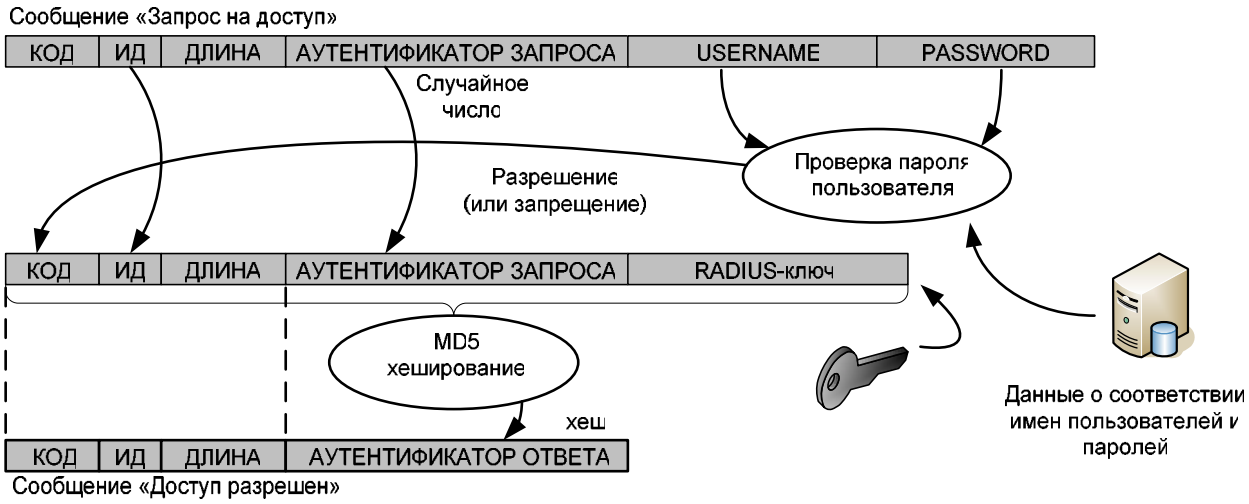


Рис. 3.4. Обработка сообщения «Запрос на доступ» протокола RADIUS

Таким образом, любое принимаемое агентом законное сообщение основывается на значении случайного числа, присутствующего в исходном сообщении.

Случайное однократно используемое число помогает агенту обнаруживать попытки воспроизведения более раннего законного ответа, посланного сервером аутентификации. Если злоумышленник воспроизводит более раннее сообщение, например корректное сообщение «Доступ разрешен» с согласующимся восьмибитовым идентификатором запроса, то хеш

аутентификатора ответа не будет выводиться из соответствующего случайного числа. Агент способен обнаружить это, повторив процесс, показанный на рис. 3.4 (исключая просмотр базы данных пользователей). Если хешированное значение, полученное в результате работы алгоритма MD5, не совпадет с хешем аутентификатора ответа, то агент отбросит сообщение как недействительное.

Вторым и более очевидным средством защиты в сообщении «Запрос на доступ» является шифрование пароля пользователя. Это не дает злоумышленнику возможности перехватить пароли пользователей в момент их прохождения между агентом и сервером аутентификации. Перед отсылкой сообщения «Запрос на доступ» агент шифрует пароль пользователя. В отличие от шифрования пароля в ОС UNIX, сервер аутентификации может провести обратную процедуру по получении сообщения «Запрос на доступ».

На рис. 3.5 показаны основные операции процедуры шифрования.

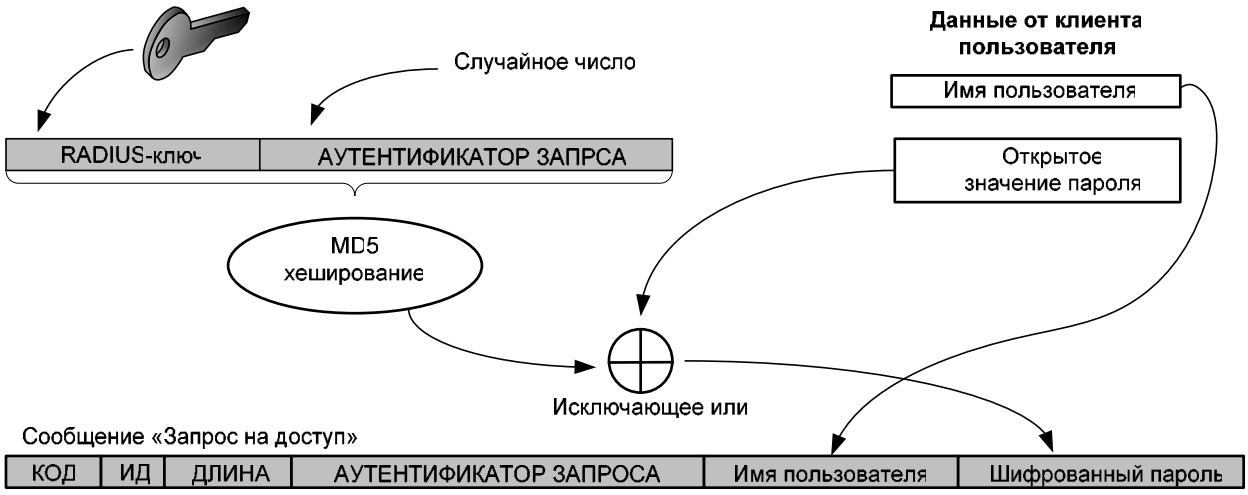


Рис. 3.5. Шифрование пароля в протоколе RADIUS

На первом этапе строится 128-разрядный ключ шифрования, для чего хешируется поле данных, содержащее базовый секрет протокола RADIUS, и случайное одноразовое число этого запроса. Чтобы получить зашифрованное значение, биты пароля объединяются с битами ключа с помощью логической

операции «исключающее или». Если пароль короче 128 бит, то он дополняется нулями. Если же он длиннее, то генерируются дополнительные ключи шифрования, что делается с помощью процедуры формирования цепочек, описанной в спецификации протокола RADIUS.

Получив сообщение, сервер аутентификации дешефрирует пароль, используя для этого ключ протокола RADIUS, которым он пользуется вместе с агентом. Сервер извлекает из сообщения «Запрос на доступ» случайное одноразовое число и объединяет его ключом протокола RADIUS, строя такой же ключ, которым пользовался агент. Процедура дешифровки аналогична процедуре шифрования: выполнение процедуры «исключающее или» над зашифрованным паролем и ключом, что в результате дает открытое значение пароля.

Может возникнуть вопрос, зачем конструировать другой ключ, объединяя его со случайным одноразовым числом, если уже имеется совместный базовый секрет в виде ключа протокола RADIUS? Во-первых, этим устраняется одно из слабых мест, связанное с использованием для шифрования операции «исключающее или». Если злоумышленникам удастся получить два или более сообщений, зашифрованных с использованием «исключающего или» с одним и тем же ключом, то они смогут легко определить зашифрованные данные. Хешируя секретный ключ и случайное однократно используемое число, получаем новый ключ всякий раз, шифруется другой пароль.

Во-вторых, эта комбинация предотвращает выполнение сложной атаки с воспроизведением. Если для шифрования пароля всегда используется один и тот же ключ, возможно, с более сильным алгоритмом шифрования, то злоумышленники могут просто скопировать зашифрованный пароль в поддельное сообщение «Запрос на доступ». И если у злоумышленников есть возможность воспроизводить пароли подобным образом, они могут обмануть сервер аутентификации и получить разрешение на вход в систему чужого пользователя. Это справедливо и при получении доступа к ресурсам сети IP-

телефонии, а также справедливо при организации атак на базы данных, биллинговые сервера и маршрутизаторы операторов. При включении в процедуру шифрования пароля случайного одноразового числа злоумышленники уже не могут повторно воспользоваться зашифрованным паролем, перехваченным из предыдущих сообщений «Запрос на доступ».

Для защиты агента от подделок и модификаций сообщений в протоколе RADIUS используется получаемое по ключу хешированное число, называемое аутентификатором ответа. Хеш вычисляется на основе содержимого ответного сообщения сервера, исключая значение аутентификатора ответа (так как это значение еще не известно), дополненного случайным одноразовым числом и ключом протокола RADIUS.

Как в случае хеширования по ключу, так и в случае хеширования аутентификатора ответа в протоколе RADIUS, значение хеша зависит от содержания сообщения и секретных данных, которые недоступны злоумышленнику. Если он каким-либо образом изменит сообщение, то получатель (т.е. агент протокола RADIUS) сможет увидеть, что значение хеша больше не соответствует содержанию сообщения. Поскольку атакующей стороне не известно значение совместно используемого секретного ключа протокола RADIUS, у нее нет возможности построить корректное значение хеша для сообщения. Как отмечалось ранее, случайное однократно используемое число предотвращает совпадение воспроизводимого сообщения с любым другим ответом сервера, посланным RADIUS-агенту.

Для максимальной безопасности каждый агент протокола RADIUS должен иметь в коллективном пользовании с сервером аутентификации уникальное значение ключа. Это позволяет владельцу системы отменять ключ протокола RADIUS того агента, на который была совершена атака и который, возможно, он был взломан, без необходимости смены ключей, используемых другими агентами. Однако, вполне обычное дело, когда на одной рабочей площадке все агенты работают с одним значением ключа протокола RADIUS, что

достаточно удобно, но до тех пор, пока в агента не было совершено проникновение, и ключ не был украден.

3.4. Выработка рекомендации по обеспечению безопасности соединения в сетях IP-телефонии.

3.4.1. Варианты доступа к услугам IP-телефонии

Если говорить о способах, к которым может прибегнуть абонент, чтобы воспользоваться услугами телефонии, то можно выделить следующие три основных варианта. Во-первых, это наиболее распространенный и хорошо всем знакомый способ подключения к сети IP-телефонии через обычный телефон. Причем он может, как поддерживать передачу DTMF сигналов, так и нет (в последнем случае пользователь прибегает к услугам оператора, который «проключает» его в указанном направлении). Вторым вариантом можно считать использование специализированных устройств – IP-телефонов. IP Ethernet-телефон – это новое устройство, которое похоже на обычный телефон, но, в отличие от него, подсоединяется к Ethernet-порту коммутатора. IP-телефон обеспечивает качество речи, сравнимое с обычным телефоном, а также имеет расширенный набор программируемых функций. У IP-телефона много общего с ПК. Он может работать как обычное IP-устройство и иметь собственный IP-адрес. Поскольку IP-телефон полностью совместим со стандартами IP-телефонии, с его помощью можно связаться с любым другим совместимым устройством или ПО, например с Microsoft NetMeeting. И, наконец, третьим вариантом может стать применение специального программного обеспечения, установленного у пользователя на его ПК (например, та же программа Microsoft NetMeeting). Если сравнивать эти варианты с существующими сценариями IP-телефонных соединений, то мы не найдем противоречий; в качестве терминала H.323 мы взяли IP-телефон и несколько расширили понятие, указав еще как вариант использование ПК с соответствующим ПО. Все дело в том, что, в основном, первый и третий

способы применяются обычными рядовыми пользователями (частными лицами, в домашних условиях), что же касается использования IP-телефонов, то сейчас к этому прибегают молодые, энергично развивающиеся компании. В связи с такой градацией, должны и вырабатываться методики обеспечения безопасности соединений в сетях IP-телефонии. Конечно, рядовой пользователь не обладает достаточными денежными средствами (по крайней мере, в той степени, в которой обладает ими любое предприятие), желанием и возможностями для создания надежной защиты своих соединений. В то время, как любая организация, постоянно пользующаяся услугами IP-телефонии и имеющая специальные программно-аппаратные средства для этого, заинтересована в сохранении конфиденциальности информации. По сравнению с рядовыми пользователями у организаций в этом плане совсем другая мотивация, и, платя определенные деньги своему провайдеру, они вправе требовать от него не только приемлемого качества, но и соответствующего уровня безопасности. В данном случае происходит столкновение двух противоположностей: рядовому пользователю, по большому счету, необходима простота использования, а не безопасность, в то время, как организации хотели, чтобы и информация оставалась в неприкосновении, в результате чего они готовы поступиться где-то простотой использования услуги.

Однако, как зачастую это бывает в случае непредвиденных обстоятельств рядовой пользователь также обращается к своему провайдеру IP-телефонии с просьбой разрешить сложившуюся ситуацию. Таким образом, пренебрегать полностью обеспечением безопасности не стоит ни в одном из трех вариантов, а что нужно делать и какими средствами этого добиться мы рассмотрим далее.

3.4.2. Доступ к сети IP-телефонии через обычный телефон.

Основная проблема, которая может возникнуть в этом случае и на предотвращение которой стоит обратить внимание провайдеру IP-телефонии – это кража сервиса. Все дело в том, что в данном случае система аутентификации носит простейший характер: пользователь указывает свой номер карты и ПИН-код, на основании которых сервер аутентификации делает вывод о том, разрешен ли доступ пользователю к ресурсам или нет. Часть проблем, связанная непосредственно с процессом аутентификации, авторизации и аудита была рассмотрена выше, в разделах, посвященных серверам аутентификации. Если вспомнить, то там предотвращение взломов рассматривалось на участке сервер доступа – сервер аутентификации, а вот про участок пользователь – сервер доступа ничего сказано не было. Здесь постараемся осветить и эту проблему.

Итак, пользователь должен знать номер карты и ПИН-код, чтобы получить доступ к ресурсам. Эти атрибуты нанесены на карту, поэтому их достаточно просто использовать, но вместе с тем, это создает и основные проблемы. Пользователь может потерять карту, или выбросить, записав в память своего телефона соответствующий набор цифр, кто-то может их подсмотреть или подслушать, когда пользователь их называет при установлении соединения через оператора. Но если в этих случаях пользователь отчасти виноват сам, то может возникнуть и другая ситуация: пользователь набирает номер карточной платформы, затем переводит свой телефон в тональный режим и, следуя указаниям автоинформатора, набирает номер своей карты и ПИН-код в режиме DTMF сигналов. В этот момент взломщик, подключившись к телефонной линии, может записать передаваемые пользователем DTMF сигналы. А затем, либо просто их проигрывая, либо преобразовав с помощью соответствующих программ в набор цифр, выдавать себя за этого пользователя.

Конечно, невнимательность и неосторожность пользователя – это ключевой момент данной проблемы, и бороться с этим провайдеру услуг IP-телефонии трудно. Именно поэтому на обратной стороне таких карт можно часто встретить надпись о том, что провайдер не несет ответственности за потерю пользователем его атрибутов, а также просит сохранять карту до тех пор, пока не будут израсходованы все средства на ней. Это действительно все так, но все равно с этим приходится постоянно сталкиваться, и поэтому какие-то механизмы все-таки нужны.

1). ***Возможность смены ПИН-кода пользователем на web-интерфейсе.*** В случае возникновения ситуации, когда атрибутами абонента воспользовалось постороннее лицо, эта функция может оказаться весьма полезной. Абонент самостоятельно заходит на сайт провайдера по гостевым параметрам и через web-интерфейс меняет ПИН-код на другой. Технически это реализуемо, причем, как правило, реализуема смена именно ПИН-кода, поскольку номер карты напрямую связан с персональным порядковым номером этой карты, который потом проходит в отчетной документации. Очевидные минусы: во-первых, не все пользователи карт IP-телефонии имеют ПК и возможность посещения этого самого web-интерфейса. Во-вторых, пользователю не нужно запоминать последовательность цифр (а это от 12 до 16 цифр), так как они занесены у него на карте; при смене ПИН-кода велика вероятность того, что пользователь забудет его. В-третьих, доступ к web-интерфейсу возможен только при вводе на сайте номера вашей карты и соответствующего ей ПИН-кода, если посторонний человек, обладая вашими реквизитами, воспользуется услугой смены ПИН-кода на web-интерфейсе, то мало того, что вы не сможете больше на него попасть, но вы не сможете и продолжать пользоваться услугами IP-телефонии, так как ваш ПИН-код уже устарел, и при аутентификации сервер будет выдавать сообщение «в доступе отказано».

Решения: при отсутствии ПК и доступа к web-интерфейсу в случае необходимости смены ПИН-кода можно обратиться по телефону в службу технической поддержки и там вам сменят его. Рекомендуется в этом случае при изготовлении карт предусматривать на обратной стороне под полем «ПИН-код» одно или два дополнительных поля, в которые пользователь сможет вписать новый ПИН-код при его смене. При невозможности попасть на свою страницу через web-интерфейс или при получении сообщения в момент авторизации, что вам отказано в доступе по причине неправильного указания номера карты или ПИН-кода свяжитесь с службой технической поддержки своего провайдера. Специалист службы техподдержки сможет определить по ряду уточняющих вопросов, кто в действительности является подлинным абонентом (например, уточнив, где была приобретена карта, или, если она проходила предварительную регистрацию, по дополнительному паролю), при этом специалист техподдержки по просьбе абонента может сделать запись в соответствующей базе данных, что при повторном обращении с таким номером карты выполнять действия (в том числе и смену ПИН-кода) только, если пользователь назовет ключевое слово, причем оно не будет видно через web-интерфейс. Таким образом, можно избежать ситуации, когда третье лицо выдает себя за пользователя, у которого уже украли реквизиты и он не может воспользоваться услугами IP-телефонии.

2.) ***Предварительная регистрация.*** Могут быть разработаны разные методики. Пользователь сам регистрирует карту на web-интерфейсе, регистрируется карта при продаже и т. д. Ощутимые минусы – это усложнение использования карт, что приведет к снижению показателей продаж, а кроме того регистрация на web-интерфейсе не дает гарантий того, что постороннее лицо не узнает дополнительный пароль, войдя на web-интерфейс по атрибутам пользователя. Причем сегодня, ПО большинства провайдеров позволяет менять такую информацию несколько раз. Теперь представим ситуацию, когда посторонний человек, войдя на страницу через web-интерфейс, меняет там

данные в поле дополнительный пароль, а затем связавшись с специалистами технической поддержки, просит запретить им какие-либо изменения, если пользователь не назовет ключевое слово. Специалист вносит это ключевое слово в базу данных и теперь оно не видно на web-интерфейсе, а злоумышленник при возможности меняет еще и ПИН-код. Теперь, когда настоящий пользователь при невозможности получения услуги свяжется с технической поддержкой, то ему вежливо во всем откажут, поскольку ключевого слова он назвать не сможет, более того все дополнительные пароли тоже, так как они изменены.

Казалось бы, логично было бы ввести обязательную регистрацию карт больших номиналов, но при продаже этим заниматься никто не будет, а продавать такие карты только в своих офисах – это терпеть большие финансовые потери.

Решения: отказаться от продажи карт больших номиналов физическим лицам (исходя из сегодняшних расценок, в среднем, на карте достаточно иметь 6 расчетных единиц, чтобы пользователь мог общаться час со странами Европы). В этом случае, при любых обстоятельствах, минимальные потери понесет как пользователь, так и провайдер в случае восполнения средств. Можно ввести, например корпоративный вариант, когда пакет карт больших номиналов предоставляется юридическим лицам. В этом случае реализовать ту же предварительную регистрацию будет значительно проще. Кроме того, в картах средних и больших номиналов можно предлагать записать по желанию ключевое слово, позвонив в службу технической поддержки, при этом специалист службы может определить подлинность абонента, уточнив, например, где была приобретена карта (в базе данных это видно, а для случайного человека информация остается недоступной) и только при положительном результате выполнить запрос. На web-интерфейсе сделать возможным только одноразовую запись дополнительного пароля.

3.) ***Приоритет оператора***. Рассмотрим следующую ситуацию: пользователь пытается установить соединение, воспользовавшись услугами оператора. В ходе выполнения запроса оператор видит, что с данными параметрами соединение уже установлено. В этом случае оператор имеет возможность по ряду дополнительных вопросов попытаться установить является ли данный пользователь настоящим или нет. Если пользователь отвечает на все вопросы верно, то оператор может войти терминальной программой на сервер доступа и сбросить установленное соединение, используя соответствующую команду, после чего посоветовать пользователю сменить ПИН-код на карте (при поддержке этой функции). Существенным минусом такой позиции является то, что увеличивается число служащих, имеющих доступ к центральной базе данных, а также имеющих право использовать специальные терминальные программы, в результате чего страдает общая сетевая политика защиты, о чем пойдет разговор в следующей главе.

Решение: заставить обращаться в подобных случаях в службу технической поддержки, специалисты которой имеют право и возможности использовать необходимые программные средства, однако, при этом значительно возрастет нагрузка на них.

4.) ***Определение пользователя по телефонному номеру или использование функции обратного вызова.*** Определение по телефонному номеру может заключаться в следующем: пользователь на web-интерфейсе указывает номер телефона, с которого он будет пользоваться услугой. При попытке авторизации сравнивается номер, с которого звонит пользователь и номер, который указан на web-интерфейсе. Очевидными недостатками является то, что номер можно легко изменить на web-интерфейсе, теряется основное преимущество таких карт – мобильность пользователя, а кроме того требуются значительные затраты оператором на соответствующее станционное оборудование (АОНы и т.д.). Услуга обратного вызова

практически нереализуема для IP-телефонии при подключении через обычный телефон и сегодня не используется, а кроме того ей присущи все недостатки, о которых говорилось при идентификации по телефонному номеру.

Вот, пожалуй, этими способами можно частично решить основную проблему доступа к сети IP-телефонии – кражу сервиса. Возможно, кто-то спросит, а как же защита информации? Но в данном случае справедливо выражение «не стоит давать больше, чем требуют». На участке пользователь – сервер доступа оператор по большому счету ответственности за защиту информации никакой не несет, а пользователь сам ее не обеспечивает. Совсем по другому обстоят дела при подключении к сети IP-телефонии другими способами.

3.4.3. Доступ к сети IP-телефонии через IP-телефон

Использование для подключения к сети IP-телефонов представляется наиболее защищенным вариантом из предложенных. Дело в том, что при их использовании, как правило в организации устанавливается маршрутизатор, в настройках которого предусмотрена возможность идентификации терминалов по IP-адресам или по локальным MAC-адресам. Канал же между маршрутизатором и RAS-сервером провайдера IP-телефонии может носить защищенный характер, но более подробно об этом будет рассказано в следующей главе. Таким образом основная ответственность за обеспечение безопасности ложится на администратора локальной сети, от провайдера же требуется поддержка соответствующих возможностей устанавливаемых маршрутизаторов (как правило, это оборудование принадлежит провайдеру, хотя и не обязательно), а также предоставление соответствующих прав администратору локальной сети.

Идентификация оборудования по MAC-адресам выглядит более надежной, чем идентификация по тем же IP-адресам, т.к. осуществить кражу IP-адреса значительно проще (об этом речь пойдет чуть дальше). Тем не менее и в том, и

в другом случае взлом уже должен происходить на территории организации, доступ на которую ограничен.

Для использования идентификации оборудования по MAC-адресам должна поддерживаться на маршрутизаторе функция защитной фильтрации портов, которая блокирует входной поток порта, когда MAC-адрес устройства, пытающегося получить к нему доступ, не совпадает со списком MAC-адресов, указанных для данного порта. Когда защищенный порт получает пакет, MAC-адрес источника пакета сравнивается с адресом надежного источника из списка, указанного в конфигурации порта. Если MAC-адрес устройства, подключенного к порту, отличается от надежного адреса, порт становится недоступным и диспетчеру SNMP посылается прерывание, соответствующее разрыву линии. Надежные MAC-адреса задаются вручную, после чего они сохраняются в энергонезависимом ЗУ.

Помимо решения проблемы несанкционированного доступа к ресурсам сети, IP-телефоны в состоянии решить и вопрос о защите информации на участке между пользователем и сервером доступа. Так, например, серия IP-телефонов компании Cisco поддерживают встроенное шифрование голосового трафика для защиты от прослушивания. Конечно, подобные методики приводят к увеличению времени между передачей сообщения и его получением на другой стороне, но при выполнении провайдером требований, предъявляемых к качеству передаваемой речи, увеличение задержек от шифровки/дешифровки информации незначительно.

3.4.4. Доступ к сети IP-телефонии с помощью программных средств

Как уже говорилось, получить доступ к ресурсам сети IP-телефонии пользователь может и при помощи программных средств, установленных у него на ПК, таких, например, как NetMeeting. При этом этот вариант доступа ориентирован в большей степени на частных пользователей. Сегодня многие имеют дома ПК, а программа NetMeeting входит в состав базовых программ

ОС Windows, поэтому вполне понятен интерес пользователей к такой альтернативе доступа к услугам IP-телефонии. Конечно, с точки зрения обеспечения безопасности такой варрант уступает использованию специальных IP-телефонов, тем более, что зачастую между пользователем и RAS-сервером средою передачи является сеть Public Internet, а не защищенные выделенные каналы, как в предыдущем случае. Но так может показаться только на первый взгляд. Да, в IP-телефонах уже изначально предусмотрены встроенные программно-аппаратные средства защиты передачи информации, но в отличие от доступа к сети IP-телефонии через обычный телефон, при использовании ПК у пользователя есть огромные возможности для того, чтобы защититься самому. Но, тем не менее, какие-то базовые возможности оборудования должен обеспечить и провайдер, чтобы при желании пользователь смог использовать защитные механизмы. Какими они могут быть?

3.4.4.1. Аутентификация PAP и CHAP

Важным моментом защиты удаленного доступа является поддержка аутентификации протоколов PAP (Password Authentication Protocol – протокол аутентификации пароля) и CHAP (Challenge Handshake Authentication Protocol – протокол аутентификации с предварительным согласованием вызова). PPP является стандартным протоколом инкапсуляции для транспортировки данных протоколов сетевого уровня (включая IP, но не ограничиваясь им) через каналы ТФОП или ISDN. Протокол PPP позволяет выполнить аутентификацию удаленных клиентов и серверов с помощью PAP и CHAP.

Аутентификация PAP при использовании протокола PPP обеспечивает удаленному клиенту простую возможность идентифицировать себя с помощью процедуры двухстороннего квитирования, которая выполняется только после установки соединения PPP. После того, как фаза установки соединения завершена, пара «имя пользователя/пароль» посылается аутентифицирующей стороне до тех пор, пока аутентификация не завершена успешно или

соединение не будет разорвано. В ходе аутентификации PAP стороны обмениваются следующими сообщениями:

1. Удаленный клиент устанавливает связь.
2. Удаленный клиент сообщает серверу сетевого доступа о том, что используется протокол PPP.
3. Сервер сетевого доступа, конфигурация которого должна допускать использование PAP, извещает удаленного клиента о применении PAP в ходе этого сеанса связи.
4. Удаленный клиент посылает имя пользователя и пароль в формате PAP.
5. Сервер сетевого доступа сравнивает имя пользователя и пароль с сохраненными в базе данных и принимает или отвергает их.

Процедура PAP не является очень надежным методом аутентификации. Имя пользователя и пароль посылаются в виде открытого текста, поэтому с помощью анализатора протокола пароль можно перехватить. Метод PAP не предлагает никакой защиты против атак воспроизведения или атак по методу проб и ошибок. Оборудование и программное обеспечение большинства поставщиков услуг поддерживают PAP, чтобы обеспечить максимальную совместимость.

Протокол CHAP предлагает более надежный метод аутентификации, чем PAP, поскольку он не предполагает передачу реального пароля по каналу связи. В CHAP для аутентификации используется процедура трехходового квитирования, которая выполняется после установки соединения и затем может повторяться периодически для гарантии аутентичности корреспондента. Процедура инициализации CHAP выполняется по схеме:

1. Соединение PPP создается в результате удаленного вызова. Конфигурация сервера сетевого доступа должна предполагать поддержку PPP и CHAP.
2. Сервер сетевого доступа предлагает удаленному клиенту использовать CHAP.

3. Удаленный клиент посылает в ответ согласие.
4. Процедура трехходового квитирования состоит из следующих шагов:
    - Сервер сетевого доступа посылает сообщение запроса удаленному клиенту;
    - Удаленный клиент возвращает значение односторонней функции хеширования;
    - Сервер сетевого доступа обрабатывает полученное значение хеширования. Если оно совпадает со значением, вычисленным сервером, аутентификация считается успешной. Пароли при этом не пересылаются.

Метод CHAP обеспечивает защиту от атак воспроизведения сообщений путем использования в запросах уникальных и непредсказуемых значений. Применение повторных запросов ограничивает время возможной атаки (повторные запросы реализуются за счет повторного использования процедуры трехходового квитирования). Таким образом, CHAP оказывается предпочтительнее PAP.

3.4.4.2. Аутентификация по телефонным номерам и IP-адресам

Сегодня многими телефонными компаниями предоставляется услуга АОН. Оператор передает эти данные на вызываемый телефон как часть сигнала вызова. Эта же технология может использоваться для аутентификации источника звонка при удаленном обращении к модему. Если компьютер запрещает соединения с неавторизованными телефонными номерами, то такой подход может защитить от подключений тех, у кого нет на это права. Проблема с подобными системами состоит в том, что система на основе использования АОН не обладает 100-процентной надежностью. Многие системы позволяют звонящему при выполнении звонка блокировать идентификатор, и это может оказать влияние на надежность информации. Возможно также, что блокировка идентификатора вызывающей стороны будет

приводить в некоторых системах к генерации вызываемой стороне сообщения с неправильными номерами, а не сообщений «номер неизвестен». Точность работы идентификаторов снижается из-за возможности проникновения злоумышленников в коммутационное оборудование телефонной компании. Таким образом, мы видим, что по большому счету, точно также как и в случае доступа к услугам IP-телефонии через обычный телефон данная система аутентификации неэффективна.

Поскольку IP-адреса задаются полностью программным обеспечением набора протоколов, обмануть программное обеспечение хост-машины и заставить его использовать неправильный адрес достаточно просто. Как правило, каждое сообщение IP-сети содержит два числовых адреса: отправителя и получателя. Если атакующая сторона хочет послать по сети сообщение, как бы посланное из другого места, то она может сконструировать его так, чтобы оно содержало желаемый адрес отправителя. В некоторых системах это вопрос лишь изменения IP-адреса хост-машины в конфигурационной информации набора протоколов. Другой подход состоит в написании специального ПО для построения сообщений и передаче таких поддельных сообщений непосредственно драйверу сетевого устройства полностью в обход набора протоколов. Хотя механизмы обработки соединений в IP-сетях позволяют противостоять некоторым простейшим подходам, основанным на подделке адресов, они не могут помешать полному перехвату IP-адреса одной хост-машины другой. При некоторых навыках можно сделать так, что бы одна машина выдала себя за другую и переключить на себя весь трафик, предназначенный для данного IP-адреса. Например, злоумышленник может сконфигурировать свой компьютер так, чтобы он имел тот же IP-адрес, что и компьютер жертвы. Если он попытается установить TCP-соединение с одним из серверов, к которым подключен обычно компьютер жертвы, то, скорее всего, сеть не сможет передать ответ квитирования на машину взломщика, так как маршрутизаторам пока не

известно, что адрес взломщика изменился. Если он продолжает настаивать, то маршрутизаторы в итоге могут обновить таблицы маршрутизации и начать рассматривать его машину как подлинную.

Злоумышленник может совершить еще более элегантную кражу адреса, используя атаку типа «человек посередине». Он устраивается в сети между жертвой и ее сервером таким образом, чтобы весь трафик жертвы проходил через этот участок сети, после чего начинает мониторинг трафика жертвы и собирает информацию, которая может ему понадобиться, чтобы взять под контроль существующее соединение. После того, как у злоумышленника оказывается нужная информация, он разрывает сетевую связь, ведущую к машине жертвы и одновременно объявляет в сети, что его машина подлинная. По сути, он сращивает TCP-соединения, а затем переключает их на свою машину. Атаки подобного типа называются TCP-сращиванием.

TCP-сращивание представляет собой пример более общей угрозы похищения соединений. Если злоумышленник может похитить соединение пользователя, то ему совсем не нужно красть его пароль доступа: он просто поджидает, пока пользователь входит в систему и затем крадет само аутентификационное соединение. Подобные вещи уже проделывались взломщиками с телефонными соединениями.

3.5. Сценарий работы безопасного VoIP-соединения

3.5.1. Общий принцип установления соединений в VoIP-сетях на базе Softswitch

В этом пункте не будут рассматриваться механизмы шифрования, криптографии и т.д., основной упор будет сделан на порядок установления соединения с точки зрения аутентификации, что укладывается в общую концепцию данной главы. На рис. 3.6 представлен общий вид сети IP-телефонии, относительно которого будем рассматривать сценарий установлении соединения.

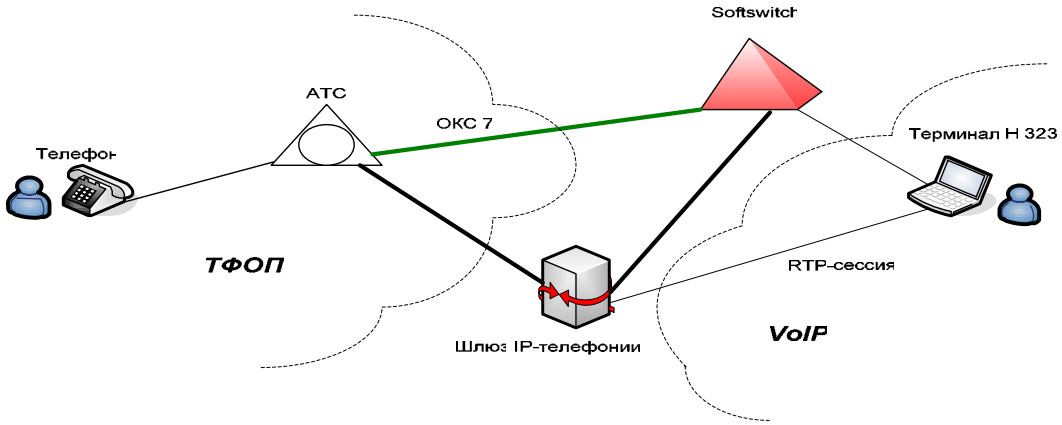


Рис.3.6. Рассматриваемая сеть IP-телефонии с использованием Softswitch

Абонент сети ТФОП (далее абонент А) снимает трубку и набирает телефонный номер, соответствующий карточной платформе IP-телефонии провайдера. АТС, к которой подключен абонент А принимает запрос и устанавливает соединение со шлюзом IP-телефонии. После этого абонент А получает голосовые подсказки со стороны оборудования провайдера, действуя согласно этим подсказкам он переводит телефон в режим тонального набора и набирает свой номер карты и ПиН-код, чтобы получить право доступа к ресурсам сети. Шлюз IP-телефонии, будучи клиентом RADIUS-сервера, передает полученные данные серверу аутентификации в сообщении Access-Request. RADIUS сервер обращается к базе данных, например Oracle, в которой хранятся данные о соответствии номеров карт и ПиН-кодов. В случае

успешной аутентификации шлюзу передается сообщение Access-Accept. После получения этого сообщения пользователю проигрываются дальнейшие подсказки и он набирает номер абонента B, который также передается RADIUS серверу для выбора тарифного плана и создания начислений. Далее шлюз передает на общеизвестный TCP порт 1720 сообщение сигнального канала H.225.0 Setup с целью установить соединение. SoftSwitch (SS) принимает запрос, обрабатывает его, анализирует адресную информацию и направляет запрос Setup либо другому шлюзу, в зоне которого находится абонент B, либо непосредственно ему, если это терминал H.323. После получения сообщения Setup происходит обмен сигнальными сообщениями RAS: ARQ и ACF между SS и оконечным оборудованием. В сообщении ARQ содержится идентификатор оборудования и alias-адрес вызывающего оборудования. В сообщении ACF указывается суммарная скорость полосы пропускания и транспортный адрес сигнального канала. Далее происходит передача сообщений вызывающей стороне H.225.0 Alerting (оборудование не занято и ему подается сигнал вызова) и Connect (содержащее транспортный адрес управляющего канала H.245). После этого между вызывающим шлюзом и вызываемым оборудованием открывается управляющий канал H.245 и происходит обмен сообщениями о функциональных возможностях оборудования TCS, определение ведущего-ведомого MSD и открытие логических каналов OLC. В сообщениях OLC содержится транспортные адреса, на которые необходимо передавать RTP-пакеты. После открытия логических каналов шлюз обменивается с RADIUS-сервером сообщениями, соответствующими началу сеанса связи.

3.5.2. Сценарий безопасной обработки вызова в сети IP-телефонии

Рассмотрим сценарий установления безопасного соединения в сети, представленной на рис. 3.6. Вопросов безопасности RTP-сесии в разговорной фазе мы коснемся чуть дальше, в Главе 4.

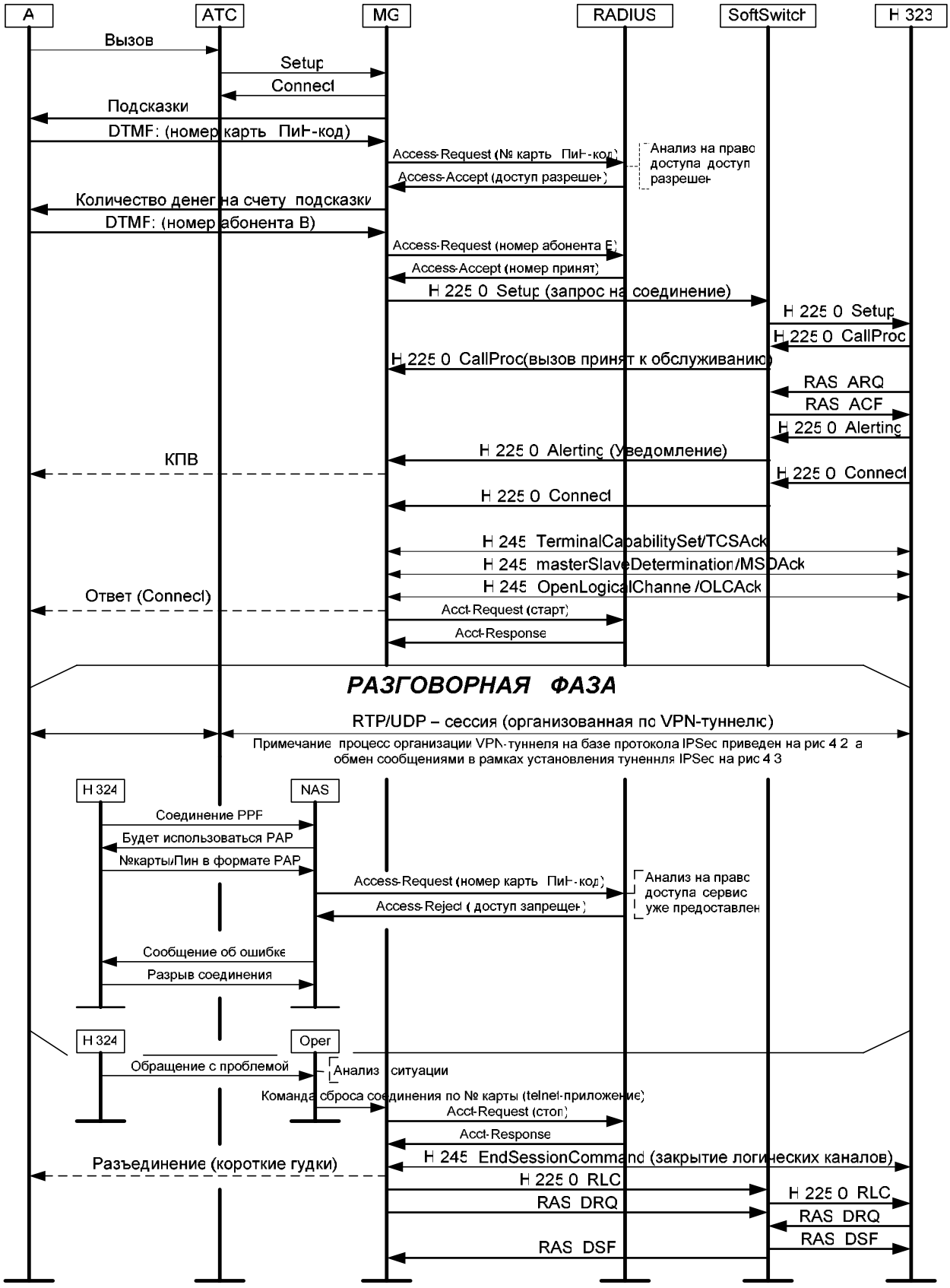


Рис.3.7. Сценарий установления безопасного соединения

1. Абонент набирает местный номер для доступа к шлюзу. Этот вызов поступает из ТФОП на шлюз через ISDN .
2. Шлюз отвечает на вызов. После голосовой подсказки, абонент набирает персональный код.
3. Шлюз (выступающий в данном случае в качестве сервера сетевого доступа) отправляет серверу RADIUS пакет Access-Request, содержащий полученные от пользователя данные для подтверждения.
4. Сервер защиты RADIUS идентифицирует посылающего клиента, выполняет аутентификацию пользователя, проверяет параметры авторизации пользователя и возвращает один из следующих ответов: Access-Accept – пользователь аутентифицирован, Access-Reject – пользователь не аутентифицирован, Access-Challenge – вызов является дополнительной возможностью сервера защиты RADIUS, позволяющей получить дополнительные данные о пользователе.
5. После того, как сервер RADIUS подтвердит, что вызывающий абонент действительно является клиентом, шлюз выдает этому абоненту второй сигнал, для набора номера.
6. Шлюз принимает набранный номер вызываемого абонента и передает его RADIUS-серверу для дальнейшего аудита.
7. Шлюз посылает SoftSwitch запрос на соединение Setup
8. SoftSwitch анализирует полученное сообщение и посылает запрос Setup терминалу H.323.
9. Softswitch и терминал H.323 обмениваются сообщениями в рамках протокола RAS: ARQ и ACF.
10. Устанавливается управляющий канал H.245, происходит обмен сообщениями в его рамках о функциональных возможностях оборудования, определения ведущего-ведомого (в данном примере роль ведущего будет отдана шлюзу) и открытие логических каналов.

11. Время начала и окончания разговора записывается на вызываемом и вызывающем шлюзах и передается на сервер RADIUS; по окончании использования сервиса шлюз посылает стоп-пакет Accounting-Request, в этом пакете указывается тип предоставленного сервиса и дополнительные статистические данные. RADIUS-сервер подтверждает получение стоп-пакета, возвращая пакет Accounting-Response.

На рис. 3.7 разрушение происходит по команде оператора, действующего по заявке некоего третьего лица, сумевшего доказать свою подлинность и тот факт, что в настоящий момент кто-то выдает себя за него, в результате чего он не может воспользоваться предоплаченной услугой.

4. Обеспечение безопасности передачи голосового трафика в сети IP-телефонии

Как мы уже отмечали, существует две проблемы в рамках обеспечения безопасности соединений в сетях IP-телефонии: это проверка прав доступа к услугам сети и непосредственно безопасность передаваемого по сети трафика. Совершенно очевидно, что для сохранения целостности и конфиденциальности сообщений необходимо использовать какие-то алгоритмы шифрования. Однако тут может возникнуть закономерный вопрос: при внедрении таких алгоритмов увеличивается и общая задержка при передаче голосовых сообщений, не повлечет ли это ухудшение связи? Формально это действительно так, однако, при обеспечении провайдером IP-телефонии соответствующего качества предоставляемого сервиса (выбор оптимального алгоритма обслуживания очередей, использование быстродействующих DSP-процессоров при обработке информации и т.д.) вносимая задержка будет не столь велика, а вот выгоду от приобретенной безопасности соединений клиенты могут получить куда как более значительную. Сегодня многие провайдеры IP-телефонии не имеют специальных выделенных сетей, предназначенных исключительно для передачи речевого трафика (как правило, совместно с IP-телефонией провайдер предоставляет и услуги доступа в Интернет, а следовательно и имеет свою IP-сеть и точки сопряжения с глобальной сетью Интернет) в результате чего разговорный трафик зачастую передается по публичной сети. Безопасность же передачи информации в таком случае внушает явное опасение. Как быть в такой ситуации?

Одним из механизмов обеспечения безопасности IP-телефонии может быть использование виртуальных частных сетей (Virtual Private Network, VPN). Существует множество вопросов сетевого планирования, касающихся сетей VPN, - например, как создать такие сети и как согласовывать их с

существующей архитектурой сети оператора. Сеть VPN является сетью предприятия, организации и т.д., разворачиваемой в рамках общедоступной инфраструктуры, но использующей возможности защиты, управления и политики качества сервиса, применяемые в частной сети. Сети VPN строятся на использовании инфраструктуры глобальных сетей, обеспечивая альтернативу существующим частным сетям, использующим арендуемые каналы. Один из возможных вариантов использования принципов VPN для передачи голосового трафика через наложенную на IP-сеть сеть VoIP-оператора представлен на рис. 4.1.

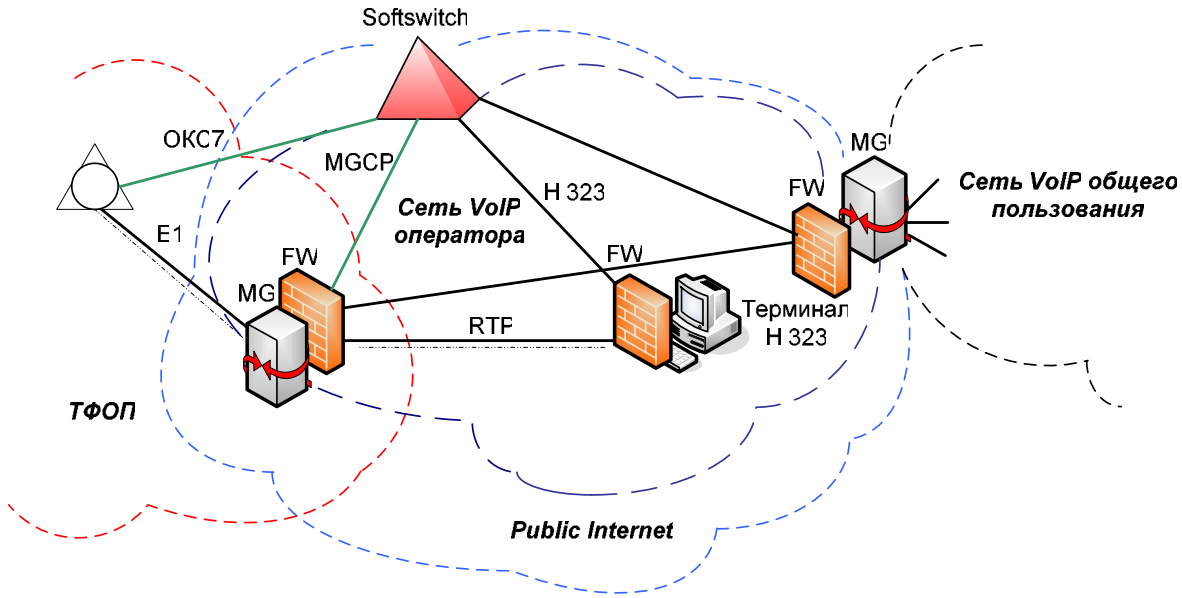


Рис. 4.1. Вариант построения сети VoIP-оператора с применением Firewall для реализации VPN-туннелей

4.1. VPN как механизм обеспечения безопасности сети IP-телефонии

Для создания сетей VPN разработано множество протоколов. Каждый из этих протоколов обеспечивает определенные возможности VPN. Например, протокол IPSec - Internet Protocol Security (упоминание об этом протоколе уже встречалось ранее, когда речь шла о безопасности в рамках рекомендации H.235) предлагает методы шифрования сетевого уровня, обеспечивающие возможности аутентификации и сервис шифрования между конечными точками в общедоступных IP-сетях. Технология IPSec и связанные с ней

протоколы защиты соответствуют открытым стандартам, которые поддерживаются группой IETF (проблемная группа проектирования Интернет) и описаны в спецификациях RFC и проектах IETF. IPSec действует на сетевом уровне, обеспечивая защиту и аутентификацию пакетов IP, пересылаемых между устройствами (сторонами) IPSec – такими как маршрутизаторы, брандмауэры Firewall, клиенты и концентраторы VPN, а также многие другие продукты, поддерживающие данный протокол.

Другие протоколы обеспечивают поддержку определенных возможностей VPN с помощью туннелирования, т.е. инкапсуляции данных или протоколов в другие протоколы. Ниже перечислены некоторые из наиболее популярных туннельных протоколов, используемых для создания сетей VPN.

- Протокол GRE (Generic Routing Encapsulation – общая инкапсуляция для маршрутизации). Разработанный Cisco туннельный протокол, обеспечивающий инкапсуляцию многих типов протокольных пакетов в туннели IP, создает виртуальную двухточечную связь с маршрутизаторами в удаленных точках IP-сети.
- Протокол L2F (Layer 2 Forwarding – протокол пересылки уровня 2). Протокол, позволяющий создать сеть VPDN – виртуальную частную коммутируемую сеть – систему, обеспечивающую существование коммутируемых сетей, распространяющихся на удаленные домашние офисы, которые кажутся при этом непосредственной частью единой сети организации.
- Протокол PPTP (Point-to-Point Tunneling Protocol – протокол туннелирования двухточечного соединения). Разработанный Microsoft сетевой протокол, обеспечивающий защищенную передачу данных от удаленного клиента к частному серверу организации с помощью создания сети VPN над IP-сетями. Протокол PPTP поддерживает маршрутизацию по требованию, многопотокольный обмен и виртуальные частные сети в открытых сетях типа Internrt.

Виртуальная частная сеть создается между инициатором туннеля и терминатором туннеля. Обычно маршрутизируемая сеть IP (она не обязательно включает в себя общедоступную сеть Интернет) определяет маршрут между инициатором и терминатором. Инициатор туннеля инкапсулирует пакеты в новый пакет, содержащий наряду с исходными данными новый заголовок с информацией об отправителе и получателе. Терминатор туннеля выполняет процесс, обратный инкапсуляции, удаляя новые заголовки и направляя исходный пакет получателю.

Сама по себе инкапсуляция никоим образом не повышает конфиденциальности или целостности туннелируемых данных. Конфиденциальность обеспечивается с помощью шифрования. Поскольку методов шифрования данных существует множество, очень важно, чтобы инициатор и терминатор туннеля использовали один и тот же метод. Кроме того, для успешного дешифрования данных они должны иметь возможность обмена ключами. Чтобы туннели создавались только между уполномоченными пользователями, конечные точки требуется идентифицировать. Целостность туннелируемых данных можно обеспечить с помощью некоей формы выборки сообщения или хэш-функции для выявления изменений или удалений.

Уже упомянутый протокол IPSec предусматривает стандартные методы идентификации пользователей или терминалов при инициации туннеля, стандартные способы использования шифрования конечными точками туннеля, а также стандартные методы обмена и управления ключами шифрования между конечными точками. Этот гибридный стандарт предлагает несколько способов для выполнения каждой задачи. Выбранные методы для одной задачи обычно не зависят от методов реализации других задач. Идентификацию можно выполнять с помощью спецификации IPSec.

IPSec может работать совместно с L2TP, в результате эти два протокола обеспечивают более надежную идентификацию, стандартизованное шифрование и целостность данных. Следует отметить наличие взаимосвязи между брандмауэрами и VPN. Если туннели завершаются на оборудовании провайдера, то трафик будет передаваться по каналу связи с провайдером в незащищенном виде.

Прокол IPSec предлагает механизм защищенной передачи данных в IP-сетях, обеспечивая конфиденциальность, целостность и достоверность данных, передаваемых через незащищенные сети. IPSec обеспечивает следующие возможности VPN:

1. Конфиденциальность данных. Отправитель данных IPSec имеет возможность шифровать пакеты перед тем, как передавать их по сети.
2. Целостность данных. Получатель данных IPSec имеет возможность аутентифицировать сообщающиеся с ним стороны (устройства или программное обеспечение, в которых начинаются или заканчиваются туннели IPSec) и пакеты IPSec, посылаемые этими сторонами, чтобы быть уверенным в том, что данные не были изменены по пути.
3. Аутентификация источника данных. Получатель данных IPSec имеет возможность аутентифицировать источник получаемых пакетов IPSec. Этот сервис зависит от сервиса целостности данных.
4. Защита от воспроизведения. Получатель данных IPSec может обнаруживать и отвергать воспроизведенные пакеты, не допуская их фальсификации и проведения атак внедрения посредника.

IPSec предлагает стандартный способ аутентификации и шифрования соединений между сообщающимися сторонами. Чтобы обеспечить защиту связей средства IPSec используют стандартные алгоритмы шифрования и аутентификации, называемыми преобразованиями. В этой концепции используются открытые стандарты согласования ключей шифрования и

управления соединениями, что обеспечивает возможность взаимодействия между сторонами. Технология IPSec предлагает методы, позволяющие сторонам «договориться» о согласованном использовании сервисов. Чтобы указать согласуемые параметры, используются ассоциации защиты.

Ассоциация защиты (Security Association – SA) представляет собой согласованную политику или способ обработки данных, обмен которыми предполагается между двумя устройствами сообщающихся сторон. Одной из составляющих такой политики может быть алгоритм, используемый для шифрования данных. Обе стороны могут использовать один и тот же алгоритм как для шифрования, так и для дешифрования. Действующие параметры SA сохраняются в базе данных ассоциаций защиты (SAD) обеих сторон. Далее под SA будем понимать данные о параметрах защиты.

Протокол IKE (Internet Key Exchange – обмен интернет-ключами) является гибридным протоколом, обеспечивающим специальный сервис для IPSec, а именно аутентификацию сторон IPSec, согласование параметров защиты IKE и IPSec. Протокол IKE опирается на протоколы ISAKMP (Internet Security Association and Key Management Protocol – протокол управления ассоциациями и ключами защиты в сети Internet) и Oakley, которые применяются для управления процессом создания и обработки ключей шифрования, используемых в преобразованиях IPSec. Как IKE, так и IPSec используют специальные сообщения в рамках согласованной политики защиты, чтобы указать параметры связи.

4.2. Основные принципы работы протокола IPSec

IPSec опирается на ряд технологических решений и методов шифрования, но действие IPSec в общем можно представить в виде следующих главных шагов:

1. Начало процесса IPSec. Трафик, которому требуется шифрование в соответствии с политикой защиты IPSec, согласованной стронами IPSec, начинает IKE-процесс.
2. Первая фаза IKE. IKE-процесс выполняет аутентификацию сторон IPSec и ведет переговоры о параметрах защиты IKE, в результате чего создается защищенный канал для ведения переговоров о параметрах защиты IPSec в ходе второй фазы.
3. Вторая фаза IKE. IKE-процесс ведет переговоры о параметрах защиты IPSec для устройств сообщающихся сторон.
4. Передача данных. Происходит обмен данными между сообщающимися сторонами IPSec, который основывается на параметрах IPSec и ключах, хранимых в базе данных сторон-участников сеанса.
5. завершение работы туннеля IPSec. Туннель IPSec завершает свою работу либо в результате удаления данных о параметрах защиты, либо по причине превышения предельного времени их существования.

На рис. 4.2 изображены пять главных шагов процесса IPSec.

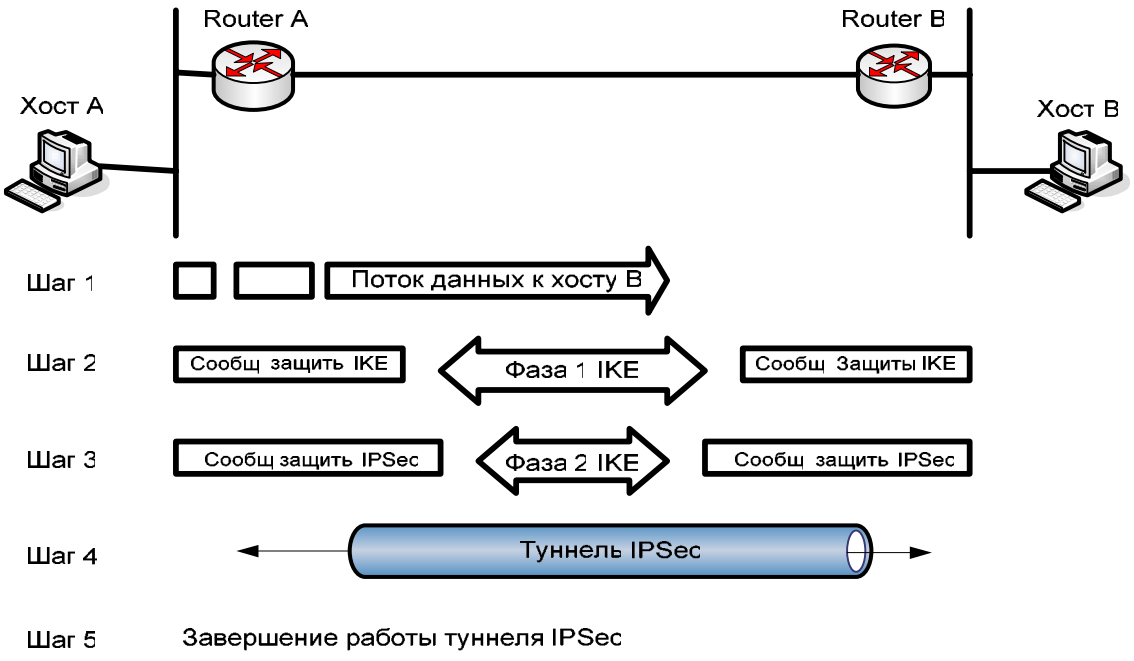


Рис.4.2. Пять шагов процесса IPSec

Шаг 1 – начало процесса IPSec. Тип трафика, который должен защищаться средствами IPSec, определяется в рамках политики защиты для VPN. Затем эта политика реализуется в виде команд конфигурации интерфейсов устройств каждой стороны IPSec. Например, в маршрутизаторах Cisco и брандмауэрах PIX Firewall для определения трафика, подлежащего шифрованию, используются списки доступа. Списки доступа реализуют политику шифрования с помощью определенных операторов (например, оператора permit), указывающих, что соответствующий трафик должен шифроваться. Когда подлежащий шифрованию трафик генерируется клиентом IPSec или проходит через него (т.е. фактически после установки RTP-сессии в случае шифрования голосового трафика в сетях IP-телефонии), клиент инициирует следующий шаг процесса, начиная первую фазу IKE.

Шаг 2 – Первая фаза IKE. Главной целью обмена данными, происходящего в первой фазе IKE, является аутентификация сторон IPSec и создание защищенного канала между сторонами, позволяющего начать обмен IKE. В ходе первой фазы IKE выполняются следующие действия:

- Ведутся переговоры о согласовании политики защиты IKE между сторонами, чтобы обеспечить защиту обмена IKE. Обмен сообщениями в рамках политики является двухсторонним и в результате участники организации туннеля IPSec получают согласованные параметры IKE
- Выполняется аутентифицированный обмен Диффи-Хеллмана, в результате которого выбирается общий секретный ключ для использования в алгоритмах шифрования IPSec.
- Выполняется аутентификация и обеспечивается защита сторон IPSec.
- Устанавливается защищенный туннель для ведения переговоров о параметрах второй фазы IKE.

Для первой фазы IKE допустимы два режима: основной и энергичный. В основном режиме выполняются три двухсторонних обмена между инициатором и респондентом:

1. В ходе первого обмена алгоритмы, используемые для защиты связи IKE, согласуются до тех пор, пока не будет достигнуто соответствие для всех ассоциаций защиты IKE сообщающихся сторон.
2. В процессе второго обмена выполняется алгоритм Диффи-Хеллмана, чтобы согласовать общий секретный материал, на основе которого создаются общие секретные ключи, передать так называемые "оказии" (случайные значения, посылаемые другой стороне), подписать их и возвратить обратно, чтобы доказать "свою личность".
3. В ходе третьего обмена выполняется аутентификация стороны – партнера. Идентификационным значением в данном случае выступает IP – адрес стороны IPSec в шифрованном виде.

Основным результатом этого режима является согласование параметров защиты IKE между сторонами с целью создания защищенного канала для последующих обменов IKE. Сообщения защиты IKE определяют параметры обмена IKE: используемый метод аутентификации, алгоритмы шифрования и хэширования, используемая группа Диффи – Хеллмана (одна из двух доступных), максимальное время существования ассоциации защиты IKE в секундах или килобайтах и совместно используемые секретные значения ключей для алгоритмов шифрования.

В энергичном режиме меньше и число обменов, и число пересылаемых при этом пакетов, в результате чего требуется меньше времени для установки сеанса IPSec. В этом случае выполняются следующие действия.

1. В ходе первого обмена почти все необходимое включается в предлагаемые значения для сообщений защиты IKE, открытый ключ Диффи-Хеллмана, оказию, подписываемую второй стороной, и пакет идентификации,

который можно использовать для того, чтобы аутентифицировать вторую сторону с помощью третьей стороны.

2. Получатель отправляет назад все, что требуется, чтобы завершить обмен. Инициатору остается только подтвердить обмен.

Недостатком использования энергичного режима является то, что обе стороны обмениваются информацией до того, как создан защищенный канал. Таким образом, можно подключиться к линии и выяснить, кто формирует новое сообщение в рамках выбранной политики защиты. С другой стороны, обмен происходит быстрее, чем в основном режиме, а в условиях передачи трафика реального времени это немаловажная особенность.

Шаг 3 – Вторая фаза IKE. Задачей второй фазы IKE является согласование параметров защиты IPSec с целью создания туннеля IPSec. В этой фазе выполняются следующие действия.

- Ведутся переговоры о параметрах защиты IPSec, защищаемые существующей ассоциацией защиты IKE.
- Устанавливается сеанс обмена сообщениями защиты IPSec.
- Периодически возобновляются переговоры о параметрах защиты IPSec, чтобы гарантировать защиту.
- В необязательном порядке может выполняться дополнительный обмен Диффи-Хеллмана.

Вторая фаза IKE выполняется только в быстром режиме, после того как в результате первой фазы IKE создается защищенный туннель. Затем ведутся переговоры о согласованной политике IPSec, извлекается общий секретный материал для работы алгоритмами защиты IPSec и происходит сеанс обмена сообщениями защиты IPSec. В быстром режиме выполняется обмен оказиями, которые обеспечивают защиту от воспроизведения сообщений. Оказии используются для того, чтобы гарантировать создание новых секретных ключей и не допустить проведение атак воспроизведения, в результате

которых злоумышленник мог бы воссоздать "фальшивый" обмен сообщениями защиты в рамках выбранной политики.

В IPSec имеется опция PFS (Perfect Forward Secrecy – совершенная прямая секретность), усиливающая защиту ключей. Если политикой IPSec предписано использование опции PFS, то для каждого обмена в быстром режиме требуется новый обмен Диффи – Хеллмана, обеспечивающий новые данные для ключей, в результате чего данные для ключей будут обладать большей энтропией ("нерегулярностью") и потому большей устойчивостью в отношении криптографических атак. Каждый обмен Диффи – Хеллмана требует большого числа возведений в степень, что увеличивает загрузку процессора и снижает общую производительность системы.

Параметры защиты, согласуемые в быстром режиме, идентифицируются IP - адресами IKE – сторон.

Шаг 4 – Передача данных. После завершения второй фазы IKE и создания ассоциаций защиты IPSec в быстром режиме, начинается обмен информацией через туннель IPSec, связывающий стороны IPSec. Пакеты шифруются и дешифруются с помощью алгоритмов шифрования и ключей, выбранных в предыдущих фазах установления туннеля IPSec. Параметры защиты IPSec задают также предел времени своего существования в килобайтах передаваемых данных или в секундах. В алгоритме защиты реализован специальный счетчик, значение которого уменьшается на единицу за каждую секунду или после передачи каждого килобайта данных.

Шаг 5 – Завершение работы туннеля IPSec. Туннель IPSec завершают свою работу либо по причине данных о параметрах защиты, либо потому, что оказывается превышен предел времени их существования. Когда происходит завершение работы, соответствующие сеансу ключи тоже становятся недействительными. Если для потока данных требуются новые параметры защиты IPSec, в рамках протокола IKE снова выполняется обмен второй фазы, а если необходимо, то и первой. В результате успешного их завершения

создаются новые данные о параметрах защиты и новые ключи. Новые данные о параметрах защиты могут создаваться и до истечения времени существования предыдущих, чтобы поток данных мог двигаться непрерывно. Обычно переговоры второй фазы выполняются чаще, чем переговоры первой фазы.

В главе 3 был рассмотрен сценарий безопасного VoIP-соединения. С учетом использования возможностей протокола IPSec для установления VPN-туннеля можно дополнить рис. 3.7 фрагментом установления защищенного туннеля. На рис. 4.3 приведен упрощенный сценарий установления и разрушения туннеля средствами протокола IPSec. Этот фрагмент соотносится с этапом сценария на рис. 3.7 отмеченным как RTP/UDP-сессия (организованная по VPN-туннелю).

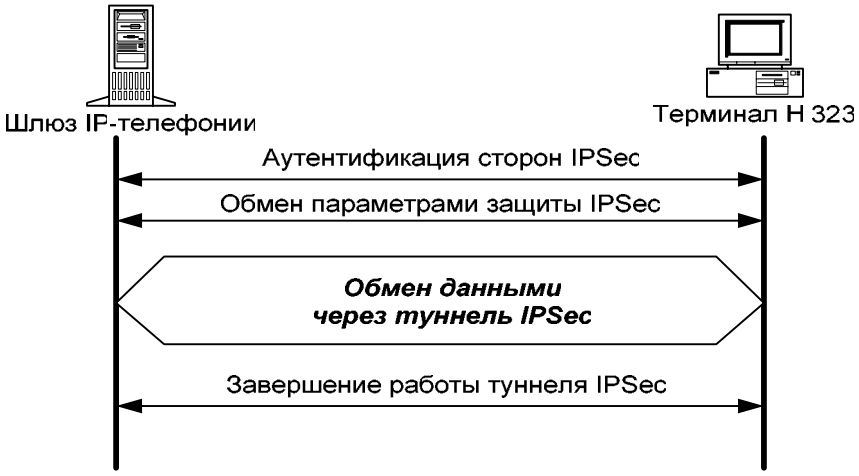


Рис. 4.3. Сценарий установления IPSec-туннеля

4.3. Согласование преобразований IPSec

В ходе второй фазы в рамках протокола IKE ведутся переговоры о преобразованиях IPSec (алгоритмах защиты IPSec). IPSec состоит из двух главных протоколов защиты и множества протоколов поддержки. Преобразования IPSec и связанные с ними алгоритмы шифрования являются следующими.

- *Протокол AH (Authentication Header - заголовок аутентификации).* Протокол – защиты, обеспечивающий аутентификацию и (в качестве опции) сервис выявления воспроизведения. Протокол AH действует как цифровая подпись и гарантирует, что данные в пакете IP не будут несанкционированно изменены. Протокол AH не обеспечивает сервис шифрования и дешифрования данных. Данный протокол может использоваться или самостоятельно, или совместно с протоколом ESP.
- *Поротокол ESP (Encapsulating Security Payload – включающий защиту полезный груз).* Протокол защиты, обеспечивающий конфиденциальность и защиту данных, а также (в качестве опции) сервис аутентификации и выявления воспроизведения. Поддерживающие IPSec продукты используют ESP для шифрования полезного груза IP - пакетов. Протокол ESP может использоваться самостоятельно или совместно с AH.
- *Стандарт DES (Data Encription Standart – стандарт шифрования данных).* Алгоритм шифрования и дешифрования данных пакетов. Алгоритм DES используется как в рамках IPSec, так и IKE. Для алгоритма DES используется 56-битовый ключ, что означает не только более высокое потребление вычислительных ресурсов, но и более надежное шифрование. Алгоритм DES является симметричным алгоритмом шифрования, для которого требуется идентичные секретные ключи шифрования в устройствах каждой из сообщающихся сторон IPSec. Для создания симметричных ключей применяется алгоритм Диффи – Хеддмана. IKE и IPSec используют алгоритм DES для шифрования сообщений.
- *"Тройной" DES (3DES).* Вариант DES, основанный на использовании трех итераций стандартного DES с тремя разными ключами, что практически утраивает стойкость DES. Алгоритм 3DES используется в рамках IPSec для шифрования и дешифрования потока данных. Данный алгоритм использует 168-битовый ключ, что гарантирует высокую надежность шифрования. IKE и IPSec используют алгоритм 3DES для шифрования сообщений.

При преобразовании IPSec используется также два стандартных алгоритма хэширования, обеспечивающих аутентификацию данных:

- *Алгоритм MD5 (Message Digest 5 – "профиль" сообщения 5).* Алгоритм хэширования, применяемый для аутентификации пакетов данных. Хэширование представляет собой процесс одностороннего (т.е. необратимого) шифрования, в результате которого для поступающего на вход сообщения произвольной длины получается вход фиксированной длины. IKE, AH и ESP используют MD5 для аутентификации данных.
- *Алгоритм SHA – 1(Secure Hash Algorithm – 1 – защищенный алгоритм хэширования1).* Алгоритм хэширования, используемый для аутентификации пакетов данных.

В рамках протокола IKE симметричные ключи создаются с помощью алгоритма Диффи-Хеллмана, использующего DES, 3DES, MD5 и SHA. Протокол Диффи – Хеллмана является криптографическим протоколом, основанным на применении открытых ключей. Он позволяет двум сторонам согласовать общий секретный ключ, не имея достаточно надежного канала связи. Так общий секретный ключ требуется для алгоритма DES. Алгоритм Диффи – Хеллмана используется в рамках IKE для создания сеансовых ключей.

Каждому набору параметров защиты IPSec присваивается индекс SPI (Security Parameter Index – индекс параметров защиты) – число, используемое для идентификации этого набора параметров защиты IPSec. Параметры защиты IPSec определяют используемое преобразование IPSec (ESP и/или AH и соответствующие алгоритмы шифрования и хэширования), предел времени существования данных о параметрах защиты IPSec в секундах или килобайтах, а также общие значения секретных ключей для алгоритмов шифрования и другие параметры.

Протоколы AH и ESP IPSec могут действовать или в туннельном, или в транспортном режимах. Туннельный режим предусматривает создание нового

заголовка IPSec. При транспортном режиме обычно используется существующий заголовок IP.

4.4. Туннельный и транспортный режимы IPSec

IPSec действует или в туннельном, или в транспортном режиме. На рис. 4.4 показана схема реализации туннельного режима. В этом режиме вся исходная дейтаграмма IP шифруется и становится полезным грузом в новом пакете IP с новым заголовком IP и дополнительным заголовком IPSec (на рис. 4.4 заголовок обозначен аббревиатурой HDR).

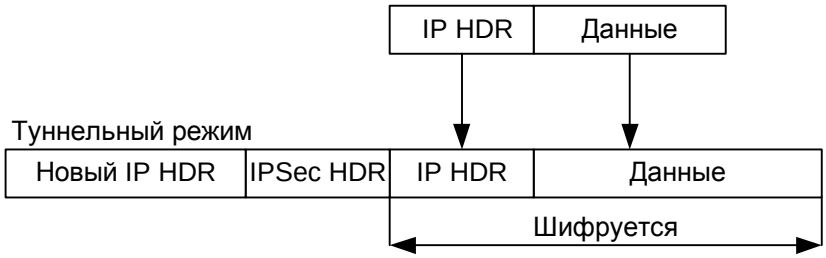


Рис. 4.4. Пакеты туннельного режима

Туннельный режим позволяет сетевому устройству (например, брандмауэру Firewall) выступать в роли шлюза IPSec или сервера, выполняющего шифрование для точек, размещенных за брандмауэром. Маршрутизатор источника шифрует пакет и передает его по туннелю IPSec. Брандмауэр Firewall адресата дешифрует полученный пакет IPSec, извлекает исходную дейтаграмму IP и передает ее системе адресата. Главное преимущество туннельного режима заключается в том, что не требуется модифицировать конечные системы, чтобы обеспечить им возможность использования IPSec. Туннельный режим также не позволяет злоумышленнику анализировать поток данных. При обмене в туннельном режиме злоумышленник имеет возможность определить только конечные точки туннеля, но не истинных источника и адресата проходящих через туннель

пакетов, даже если конечные точки туннеля находятся как раз в системах источника и адресата.

Схема на рис. 4.5 иллюстрирует транспортный режим.

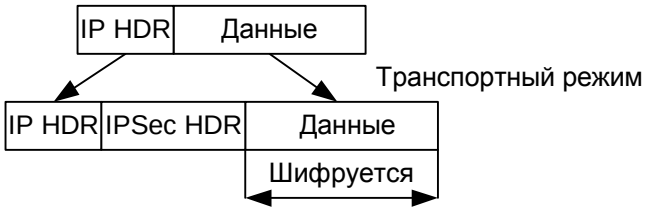


Рис.4.5. Транспортный режим

Здесь шифруется только полезный груз IP, а исходный заголовок IP остается нетронутым. Добавляется заголовок IPSec. Преимуществом этого режима является добавление только нескольких байтов к каждому пакету. Кроме того, устройства открытой сети могут видеть истинные адреса отправителя и получателя пакета. Это позволяет использовать специальные возможности промежуточных сетей (например, гарантированное качество сервиса), основанные на информации в заголовке IP. Однако заголовок уровня 4 шифруется, что ограничивает возможности анализа пакета. К сожалению, передача заголовка IP в открытом виде в транспортном режиме позволяет злоумышленнику в определенной мере выполнить анализ потока данных. Например, он может выяснить, сколько пакетов было передано сторонами IPSec, действующими в транспортном режиме. Но злоумышленник может узнать только о том, что пакеты IP пересылались. Он не сможет определить, что это за сообщения, если использовался протокол IPSec.

4.5. Атаки на компоненты IPSec

Все виды атак на компоненты IPSec можно разделить на следующие группы: атаки, эксплуатирующие конечность ресурсов системы (типичный пример - атака "Отказ в обслуживании”), атаки, использующие особенности и

ошибки конкретной реализации IPSec и, наконец, атаки, основанные на слабостях самих протоколов AH и ESP, на которых основан весь принцип IPSec. Отдельно криптографические атаки можно не рассматривать - оба протокола определяют понятие "трансформ", куда скрывают всю криптографию. Если используемый криптоалгоритм стоек, а определенный с ним трансформ не вносит дополнительных слабостей (это не всегда так, поэтому правильнее рассматривать стойкость всей системы - Протокол-Трансформ-Алгоритм), то с этой стороны все нормально. Что остается? Replay Attack - нивелируется за счет использования Sequence Number (в одном единственном случае это не работает - при использовании ESP без аутентификации и без AH). Далее, порядок выполнения действий (сначала шифрация, потом аутентификация) гарантирует быструю отбраковку "плохих" пакетов (более того, согласно последним исследованиям в мире криптографии, именно такой порядок действий наиболее безопасен, обратный порядок в некоторых, правда очень частных случаях, может привести к потенциальным дырам в безопасности; к счастью, ни SSL, ни IKE, ни другие распространенные протоколы с порядком действий "сначала аутентифицировать, потом зашифровать", к этим частным случаям не относятся, и, стало быть, этих дыр не имеют). Остается Denial-Of-Service атака. Как известно, это атака, от которой не существует полной защиты. Тем не менее, быстрая отбраковка плохих пакетов и отсутствие какой-либо внешней реакции на них (согласно RFC) позволяют более-менее хорошо справляться с этой атакой. В принципе, большинству (если не всем) известным сетевым атакам (sniffing, spoofing, hijacking и т.п.) AH и ESP при правильном их применении успешно противостоят. С IKE несколько сложнее. Протокол очень сложный, тяжел для анализа. Кроме того, в силу опечаток при его написании и не совсем удачных решений он содержит несколько потенциальных "дыр" (в частности, в первой фазе не все сообщения в сообщении аутентифицируются), впрочем, они не очень серьезные и ведут,

максимум, к отказу в установлении соединения. От атак типа replay, spoofing, sniffing, hijacking IKE более-менее успешно защищается. С криптографией несколько сложнее, - она не вынесена, как в AH и ESP, отдельно, а реализована в самом протоколе. Тем не менее, при использовании стойких алгоритмов и примитивов (PRF), проблем быть не должно. В какой-то степени можно рассматривать как слабость IPsec то, что в качестве единственного обязательного к реализации криптоалгоритма в нынешних спецификациях указывается DES (это справедливо и для ESP, и для IKE), 56 бит ключа которого уже не считаются достаточными. Тем не менее, это чисто формальная слабость - сами спецификации являются алгоритмо-независимыми, и практически все известные вендоры давно реализовали 3DES (а некоторые уже и AES).Таким образом, при правильной реализации, наиболее "опасной" атакой остается Denial-Of-Service.

Оценка протокола. Протокол IPSec получил неоднозначную оценку со стороны специалистов. С одной стороны, отмечается, что протокол IPSec является лучшим среди всех других протоколов защиты передаваемых по сети данных, разработанных ранее (включая разработанный Microsoft PPTP). По мнению другой стороны, присутствует чрезмерная сложность и избыточность протокола. Так, Niels Ferguson и Bruce Schneier в своей работе "A Cryptographic Evaluation of IPsec" отмечают, что они обнаружили серьёзные проблемы безопасности практически во всех главных компонентах IPsec. Эти авторы также отмечают, что набор протоколов требует серьёзной доработки для того, чтобы он обеспечивал хороший уровень безопасности. В работе приведено описание ряда атак, использующих как слабости общей схемы обработки данных, так и слабости криптографических алгоритмов.

ЗАКЛЮЧЕНИЕ

В дипломной работе был дан анализ обеспечения безопасности соединения в сетях IP-телефонии. Были проанализированы возможности протоколов IP-телефонии с точки зрения обеспечения безопасности, было приведено сравнение двух наиболее популярных протоколов аутентификации TACACS+ и RADIUS, проанализирован вариант защиты информации в канале за счет использования технологии виртуальных частных сетей на базе протокола IPSec. Как результат, была выработана рекомендация по обеспечению безопасности соединения в сетях IP-телефонии и представлен сценарий установления безопасного VoIP-соединения. В работе были смоделированы и рассмотрены различные атаки на сеть IP-телефонии и предложены варианты защиты. Выработанные алгоритмы в целом удовлетворяют защите от смодулированных ситуаций.

Приведенный анализ указывает на необходимость внедрения эффективных механизмов защиты соединений в сетях IP-телефонии для того, чтобы провайдер оставался конкурентоспособным на растущем рынке телематических услуг. Для чего в рамках обеспечения безопасности с точки зрения несанкционированного доступа рекомендуется использование протокола RADIUS, а с точки зрения обеспечения конфиденциальности и целостности информации, передаваемой в каналах сети IP-телефонии технологии IPSec.

ЛИТЕРАТУРА

1. Амато В. Основы организации сетей Cisco. Том 1. М.: издательский дом «Вильямс», 2002.
2. Амато В. Основы организации сетей Cisco. Том 2. М.: издательский дом «Вильямс», 2002.
3. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP телефония. М.: Радио и связь, 2001.
5. Лукацкий А.В. Атаки на VPN. «Компьютер-Пресс», №3. 2002.
6. Лукацкий А.В. IP-опасность для бизнеса. «Мир связи. Connect», N8. 2002.
7. Лукацкий А.В. Системы обнаружения атак. «Сетевой», №4. 2002.
8. Олифер В.Г., Олифер Н.А. Компьютерные сети. СПб.: Питер, 2002.
9. Росляков А.В., Самсонов М.Ю., Шибаева И.В. IP телефония. М.: Эко-Трендз, 2003.
10. Смит Ричард Э. Аутентификация: от паролей до открытых ключей. М.: издательский дом «Вильямс», 2002.
11. Столлинз Вильям. Криптография и защита сетей. Принципы и практика. 2-е издание. М.: издательский дом «Вильямс», 2002.
12. Уэнстром Майкл. Организация защиты сетей Cisco. М.: издательский дом «Вильямс», 2003.
13. Материалы сайта НПО Информ-защита http://www.infosec.ru
14. Материалы сайта НИИ Телекоммуникационных систем http://www.niits.ru

ПЛАКАТ 1. ТЕМА ДИПЛОМНОЙ РАБОТЫ. ЦЕЛИ. ЗАДАЧИ.

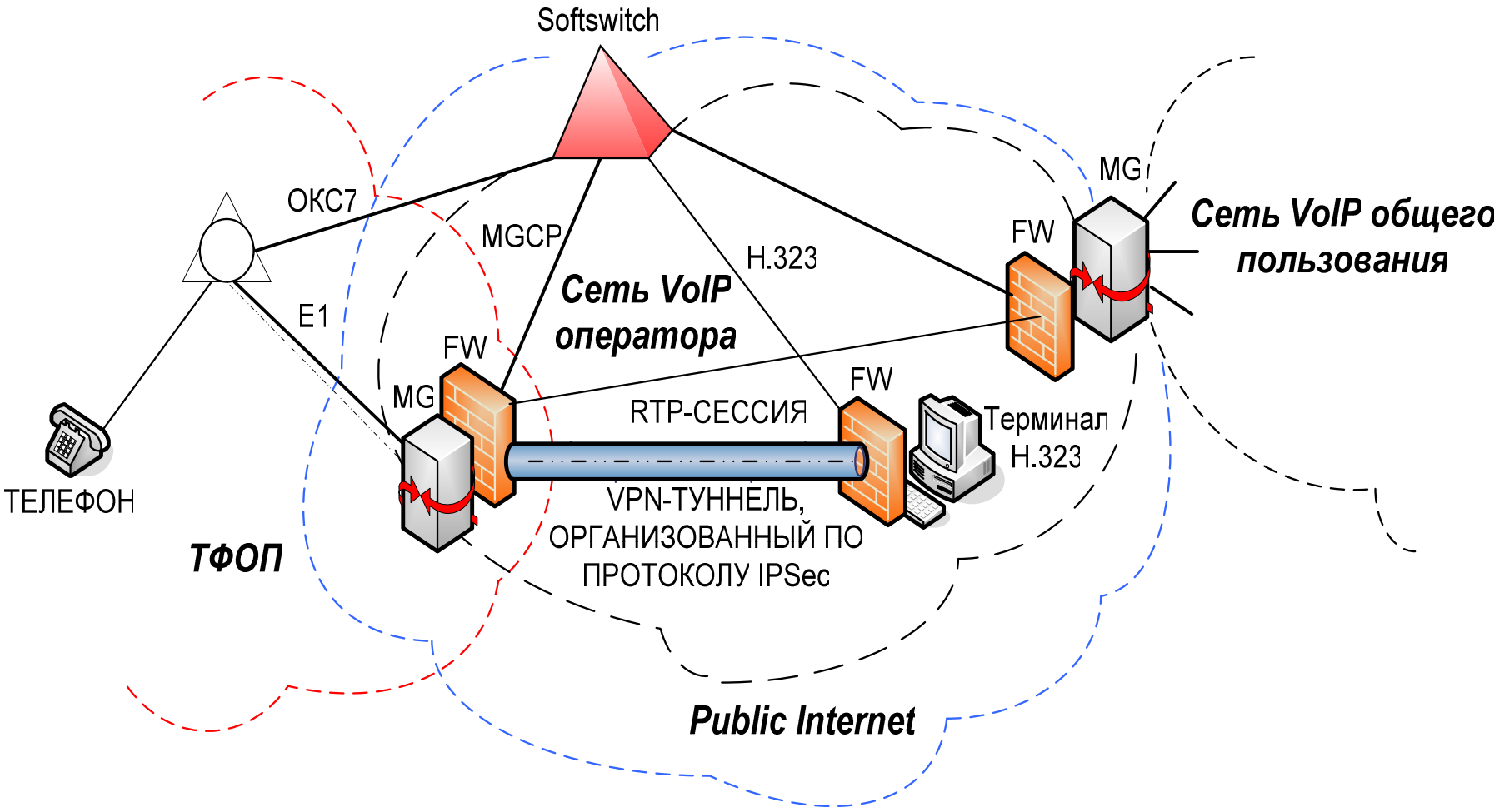
Тема работы: «Анализ проблем обеспечения безопасности соединений в сетях IP-телефонии»

Цель: Проанализировать слабые места сети IP-телефонии с точки зрения проблем обеспечения безопасности соединений и предложить возможные способы их устранения.

Задачи:

- Проанализировать возможности протоколов IP-телефонии с точки зрения заложенных алгоритмов, направленных на обеспечение безопасности соединений.
- Обосновать выбор оптимального протокола аутентификации, авторизации и учета, исходя из требований сети IP-телефонии.
- Указать на слабые места процессов аутентификации, авторизации и учета в рамках обеспечения безопасного доступа к ресурсам сети. Проанализировать возможные варианты атак в связи с этим и механизмы по их предотвращению, заложенные в выбранном протоколе.
- Смоделировать ряд ситуаций, попадающих под категорию атак на сеть IP-телефонии, и предложить механизмы их разрешения. На основе предложенных механизмов выработать рекомендацию по обеспечению безопасности соединений в сетях IP-телефонии.
- Рассмотреть проблему безопасности соединений с точки зрения обеспечения безопасности информации непосредственно в каналах сети IP-телефонии. Предложить возможный вариант защиты информации и проанализировать технологии и протоколы, используемые для его реализации.

ПЛАКАТ 2. СТРУКТУРА ЗАЩИЩЕННОЙ VoIP-СЕТИ



ПЛАКАТ 3. АТАКИ НА СЕТЬ IP-ТЕЛЕФОНИИ И МЕХАНИЗМЫ БОРЬБЫ С НИМИ

1.Отказ в обслуживании:

- Ведение списка полуоткрытых соединений в порядке поступления запросов и отбрасывании более старых при поступлении новых запросов;
- Использование списков доступа.

2. Подмена номера:

- Использование эффективных механизмов аутентификации;
- Использование соответствующих фильтров и систем обнаружения вторжений.

3. Перехват данных:

- Шифрование данных;
- Применение целых концепций построения сети IP-телефонии, в которых в частности заложены и алгоритмы шифрования. Такой концепцией может быть, например, использование VPN-туннелей.

4. Кража сервиса:

- 128-разрядное случайное число в сообщениях протокола RADIUS;
- Шифрование пароля пользователя в протоколе RADIUS.

При использовании предоплаченных карт доступа к услугам IP-телефонии провайдером должны быть предусмотрены следующие механизмы, препятствующие краже сервиса:

- Возможность смены ПИН-кода пользователем на web-интерфейсе;
- Предварительная регистрация карт;
- Приоритет оператора;
- Определение пользователя по телефонному номеру или использование функции обратного вызова.

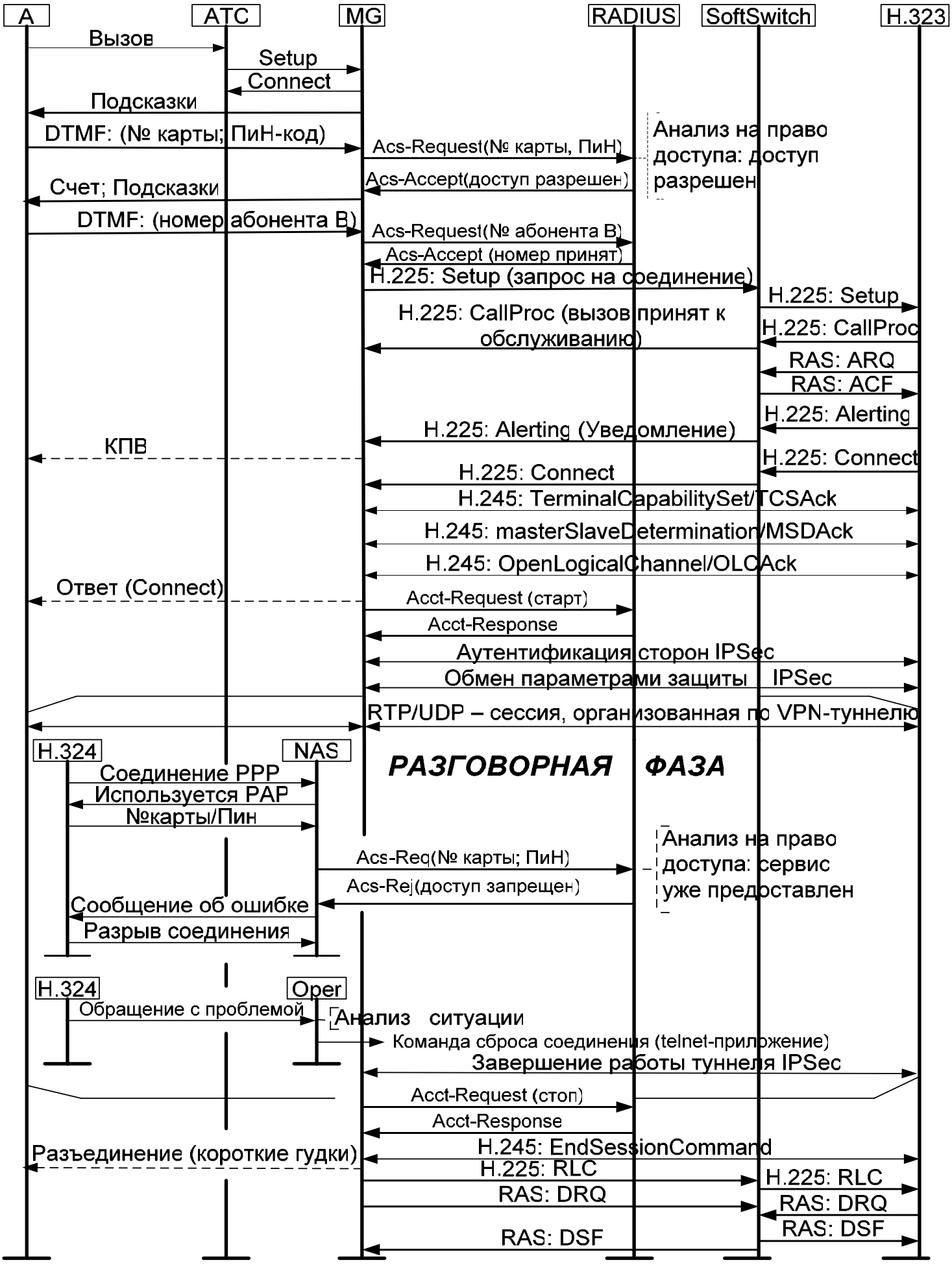
ПЛАКАТ 4. СРАВНЕНИЕ ПРОТОКОЛОВ TACACS+ И RADIUS

Функциональные возможности	TACACS+	RADIUS
Поддержка AAA	Разделение трех сервисов AAA	Аутентификация и авторизация объединяются, а аудит отделяется
Транспортный протокол	TCP	UDP
Обмен сообщениями между клиентом и сервером защиты	Двунаправленный	Однонаправленный
Поддержка протоколов удаленного и межсетевого доступа	Полная поддержка	Отсутствует поддержка NetBEUI
Целостность данных	Шифруется весь пакет TACACS+	Шифруются только пароли пользователей
Возможность перенаправления запроса	Нет	Есть

Кроме того, следует отметить следующую особенность протоколов:

- *Гарантия доставки* обеспечивается тем, что для обработки запроса TACACS+ сервер и клиент должны установить TCP-соединение, а с точки зрения времени это довольно длительный процесс. В протоколе RADIUS при потере пакета используется его повторная отправка, что снижает временные показатели при обработке запросов.

ПЛАКАТ 5. СЦЕНАРИЙ БЕЗОПАСНОГО VoIP-СОЕДИНЕНИЯ



Рецензия
на дипломную работу студента гр. СК – 95
Щербакова Дмитрия Николаевича
на тему: «Анализ проблем обеспечения безопасности соединений в сетях IP-телефонии».

Актуальность темы обусловлена открывающимися сегодня перспективами использования услуг IP-телефонии. Для того, чтобы оставаться конкуренто-способными на рынке телекоммуникационных услуг, провайдеры IP-телефонии должны учитывать все возрастающие потребности пользователей. На данный момент пользователей в большей степени интересует качество связи и безопасность соединений.

Главными вопросами, освещенными в дипломной работе, являются моделирование ситуаций, влекущих угрозу безопасности предоставления услуг IP-телефонии, их анализ и обзор методов по их предотвращению. В ходе выполнения дипломной работы выработана рекомендация по обеспечению безопасности соединений в сетях IP-телефонии.

Таким образом, рассматриваемая работа представляет практическую ценность, а отдельные предложения, изложенные в рекомендации, могут быть интересны провайдерам IP-телефонии.

Вместе с тем следует отметить, что работа не лишена некоторых недостатков:

- отсутствуют ссылки на использованную литературу;
- не упомянуты альтернативные методики, протоколы и технологии, например, туннелирование MPLS, SSL и т. д.

Дипломная работа может быть оценена «отлично», а ее автор Щербаков Д.Н. заслуживает звания инженера по специальности «Сети связи и системы коммутации».

Рецензент
Ст. преподаватель каф. Сетей связи О.А.Симонина

Отзыв
на дипломную работу студента
факультета СС, СК и ВТ
СПбГУТ им. проф. М.А. Бонч-Бруевича
Щербакова Дмитрия Николаевича
на тему: «Анализ проблем обеспечения безопасности соединений в сетях IP-телефонии»

Несмотря на то, что IP-телефония пока еще достаточно новая технология со всеми своими плюсами и минусами, уже сегодня ей предпочтение отдают не только отдельные пользователи, но и малые и средние предприятия. Вместе с тем, по ряду ключевых вопросов к IP-телефонии на данный момент остается ряд претензий, в том числе и в вопросах обеспечения безопасности соединений. Пользователям, особенно это касается бизнес клиентов, зачастую действительно необходима такая безопасность. Поэтому тема дипломной работы представляется на сегодня актуальной и интересной, причем не только для специалистов в области телекоммуникаций, но и для обычных пользователей услугами IP-телефонии, что обусловлено во многом доступностью языка изложения.

В целом, в ходе работы были раскрыты вопросы, поставленные в техническом задании, для чего использовалась актуальная и современная литература за последние несколько лет. Положительной чертой работы следует считать выработанную рекомендацию по обеспечению безопасности соединения в сетях IP-телефонии, отдельные моменты которой уже сейчас могли бы взять себе на вооружение провайдеры. В работе были смоделированы реальные ситуации угрозы безопасности соединений в сетях IP-телефонии, проанализированы и предложены механизмы их устранения.

Дипломная работа отвечает всем предъявленным требованиям и заслуживает отличной оценки, а Щербаков Дмитрий Николаевич достоин присвоения квалификации инженера по специальности "Сети связи и системы коммутации".

Руководитель
Начальник сектора ЛОНИИС Гольдштейн А. Б.