IP-телефония? Ее тоже атакуют!

IP-телефония (VoIP) сейчас переживает бум - о ней говорят все и вся, расписывая ее несомненные достоинства (сокращение расходов за междугородние и международные переговоры, возможность совместной передачи данных и голоса по одним физическим каналам связи, интеграция с различными приложениями и т.д.). Но как быть с безопасностью IP-телефонии? 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.

Принцип действия

Принцип действия технологии IP-телефонии прост. Центральным ее компонентом является сервер (шлюз), который отвечает за соединение телефонной и IP сетей, т.е. он подключен как к телефонной сети и может дозвониться до любого обычного телефона, так и к сети передачи данных (например, Internet) и может получить доступ к любому компьютеру. В функции данного устройства входят:

- Ответ на вывоз вызывающего абонента
- Установление соединение с удаленным шлюзом и вызываемым абонентом
- Оцифровка (кодирование), сжатие, разбиение на пакеты и восстановление сигнала

Данный шлюз (например, Cisco Catalyst 4000 Access Gateway Module или Cisco VG200) на вход принимает обычный телефонный сигнал, оцифровывает его (если сигнал не цифровой) и проводит сжатие полученных данных, после чего передает в IP-сеть в виде обычных пакетов (но не очень большого размера). На другом конце шлюз восстанавливает сигнал в обратном порядке. Данный компонент может и не использоваться, если вы не планируете интегрировать свои IP-телефоны в телефонную сеть общего пользования (см. рис.1).

Для того чтобы можно было построить распределенную сеть IP-телефонии необходимо наличие диспетчера, который отвечает за распределение вызовов между шлюзами (например, Cisco CallManager). Помимо этой задачи диспетчер проводит аутентификацию и авторизацию абонентов, а также обладает интерфейсом к биллинговой системе.

Для удобства администрирования большого числа удаленных шлюзов и диспетчеров может использоваться специальное программное обеспечение, называемое монитором. Ну и, наконец, последним обязательным элементом сети IP-телефонии является абонентский пункт, который может быть реализован как программным (например, Cisco IP SoftPhone), так и аппаратным способом (например, Cisco IP Phone, подключаемые напрямую к Ethernet-порту коммутатора). Причем в первом случае звонки можно осуществлять даже через домашний компьютер, оснащенный звуковой картой и микрофоном, а во втором случае, в качестве абонентского пункта выступает т.н. IP-телефон.

Еще одним компонентом архитектуры IP-телефонии можно назвать специализированные пользовательские приложения, возникшие благодаря интеграции голоса, видео и данных (call-центры, системы унифицированной обработки сообщений).

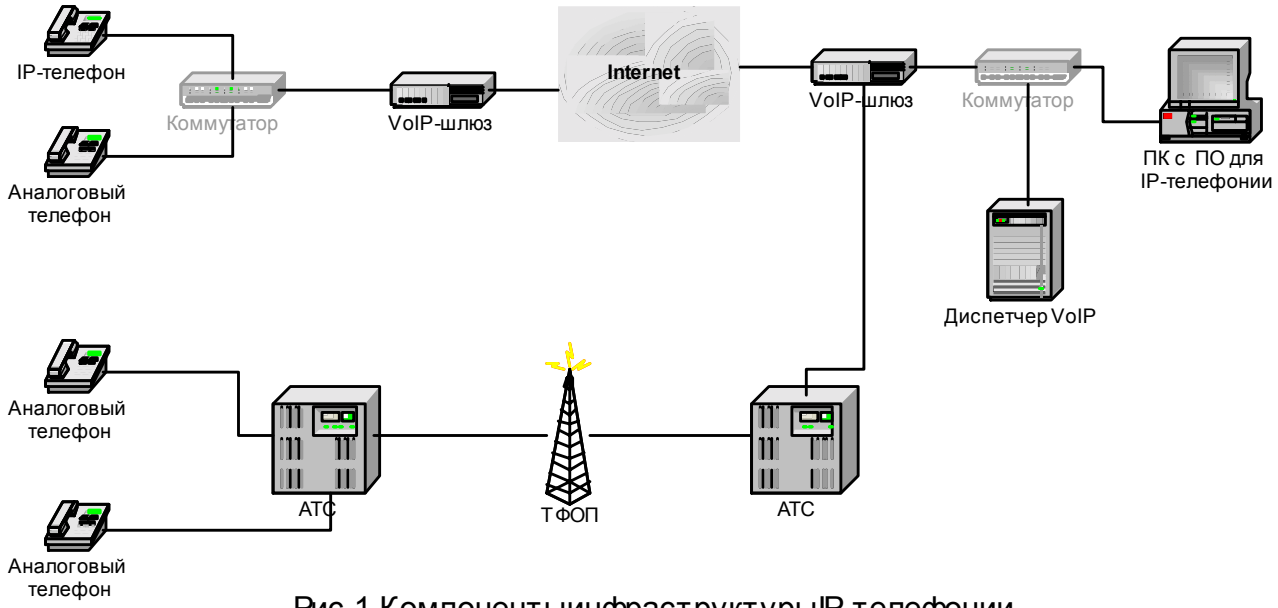

Рис.1.Компонентыинфраструктуры IP-телефонии

Зачем атакуют IP-телефонию?

Сети IP-телефонии – хорошая цель для хакеров. 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. Ваши конкуренты могут захотеть подорвать вашу репутацию путем выведения из строя шлюзов и диспетчеров, тем самым, нарушая доступность телефонных услуг для ваших абонентов, что, в свою очередь, может также привести к нанесению ущерба бизнесу ваших клиентов. Существуют и другие причины, например, звонки за чужой счет (кража сервиса).

Возможные угрозы

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 нам и пути их защиты, но об этом чуть дальше.

Атаки на обычную телефонию применимы и для ее IP-родственницы - фонарь.

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. Перечислю некоторые из них, часть их которых я рассмотрю более подробно:

- Подслушивание телефонных переговоров
- Отказ в обслуживании
- Подмена номера
- Кража сервисов
- Неожидаемые вызовы
- Несанкционированное изменение конфигурации
- Мошенничество со счетом.

Перехват данных

Перехват данных – самая большая проблема, как обычной телефонии, так и ее IP-родственницы. 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. Таким грехом страдают HTTP, SMTP, IMAP, FTP, Telnet, SQL*net 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 сразу хочу 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. - фонарь

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. Именно поэтому задача обеспечения аутентификации не обойдена вниманием во всех существующих VoIP-стандартах и будет рассмотрена чуть позже.

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. Например, Internet-черви Red Code, Nimda, различные троянцы и вирусы, DoS-атаки и их распределенные модификации – все это способно, если не вывести из строя голосовую IP-инфраструктуру, то существенно нарушить ее функционирование. 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 букетом дыр.

Атаки на диспетчеры

Злоумышленники могут атаковать и узлы (Gatekeeper в терминах H.323 или Redirect server в терминах SIP), 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.

Стандарты IP-телефонии и механизмы их безопасности

Отсутствие единых принятых стандартов в данной области (см. рис.2) не позволяет разработать и универсальные рекомендации по защите устройств IP-телефонии. Каждая рабочая группа или производитель по-своему решает задачи обеспечения безопасности шлюзов и диспетчеров, что приводит к необходимости тщательного их изучения перед выбором адекватных мер по защите.

Безопасность H.323

H.323 - протокол, который позволяет построить VoIP-систему от начала и до конца. H.323 включает в себя ряд спецификаций, в т.ч. и H.235, которая реализует некоторые механизмы безопасности (аутентификацию, целостность, конфиденциальность и невозможность отказа от сообщений) для голосовых данных.

Аутентификация в рамках стандарта H.323 может быть реализована как с помощью алгоритмов симметричной криптографии (в этом случае не требуется никакого предварительного обмена между взаимодействующими устройствами и не так интенсивно нагружается центральный процессор), так и с помощью сертификатов или паролей. Кроме того, спецификация H.235 позволяет использовать в качестве механизма аутентификации IPSec, который также рекомендуется к применению и в других стандартах IP-телефонии.

После установки защищенного соединения, которое происходит через 1300 tcp-порт, узлы, участвующие в обмене голосовыми данными, обмениваются информацией о методе шифрования, которое может быть задействовано на транспортном (шифрование пакетов RTP-протокола) или сетевом (с помощью IPSec) уровне.

Безопасность SIP

Данный протокол, похожий на HTTP и используемый абонентскими пунктами для установления соединения (не обязательно телефонного, но и, например, для игр), 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. Кстати, компания Cisco в своей архитектуре безопасности корпоративных сетей SAFE, очень большое внимание уделяет практическим вопросам защиты IP-телефонии.

Безопасность MGCP

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).

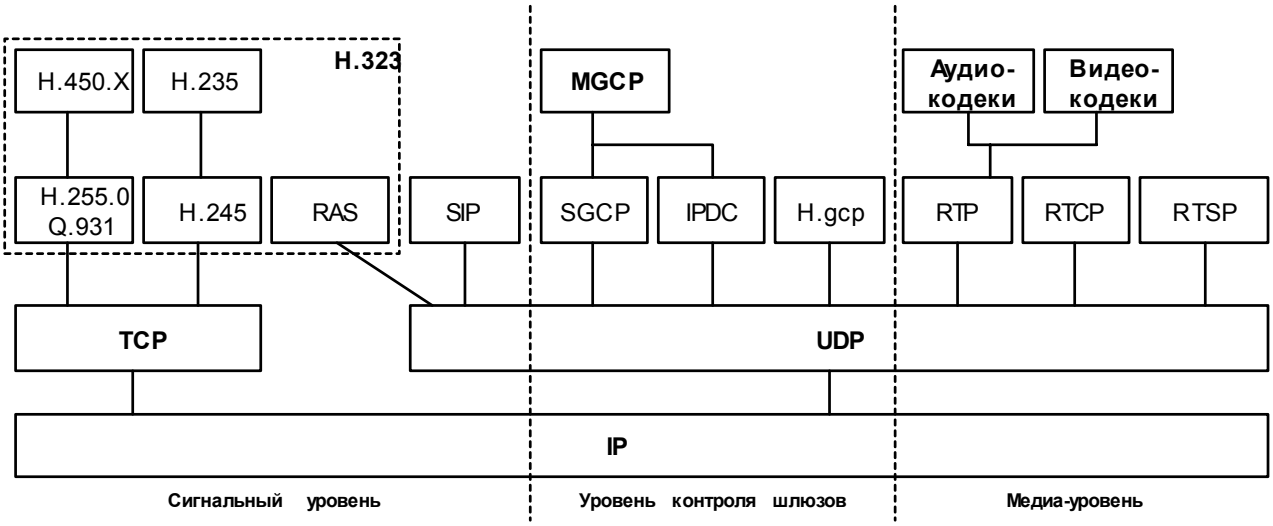

Рис.2.Архитектурапротоколов IP-телефонии

Обеспечение безопасности

Выбор правильной топологии

Не рекомендуется использовать для VoIP-инфраструктуры концентраторы, которые облегчают злоумышленникам перехват данных. Кроме того, т.к. оцифрованный голос обычно проходит по той же кабельной системе и через тоже сетевое оборудование, что и обычные данные, стоит правильно разграничить между ними информационные потоки. Это, например, может быть сделано с помощью механизма VLAN (однако не стоит полагаться только на них). Сервера, участвующие в инфраструктуре IP-телефонии желательно размещать в отдельном сетевом сегменте (см. рис.3), защищенном не только с помощью встроенных в коммутаторы и маршрутизаторы механизмов защиты (списки контроля доступа, трансляция адресов и обнаружение атак), но и с помощью дополнительно установленных средств защиты (межсетевые экраны, системы обнаружения атак, системы аутентификации и т.д.).

Вы должны помнить, что передача голосовых данных по вашей корпоративной сети накладывает на ее проектирование особый отпечаток. Большое внимание вы должны уделить вопросам высокой доступности и отказоустойчивости. Если пользователи еще могут привыкнуть к непродолжительному выходу из строя Web-сервера или почтовой системы, то привыкнуть к нарушению телефонной связи они не смогут. Обычная телефонная сеть так редко выходит из строя, что многие пользователи закономерно наделяют свойством безотказности и ее IP-сестру. Поэтому сбой в работе VoIP-инфраструктуры может подорвать к ней доверие со стороны пользователей, что в свою очередь может привести к отказу от ее использования и нанесению материального ущерба ее собственнику.

Физическая безопасность

Желательно запретить неавторизованный доступ пользователей к сетевому оборудованию, в т.ч. и коммутаторам, и по возможности все неабонентское оборудование разместить в специально оборудованных серверных комнатах. Это позволит предотвратить несанкционированное подключение компьютера злоумышленника. Кроме того, следует регулярно проверять наличие несанкционированно подключенных к сети устройств, которые могут быть "врезаны" напрямую в сетевой кабель. Для определения таких устройств можно использовать различные методы, в т.ч. и сканеры (например, Internet Scanner или Nessus), дистанционно определяющие наличие в сети "чужих" устройств.

Контроль доступа

Еще один достаточно простой способ защиты инфраструктуры VoIP – контроль MAC-адресов. Не разрешайте IP-телефонам с неизвестными MAC-адресами получать доступ к шлюзам и иным элементам IP-сети, передающей голосовые данные. Это позволит предотвратить несанкционированное подключение «чужих» IP-телефонов, которые могут прослушивать ваши переговоры или осуществлять телефонную связь за ваш счет. Разумеется, MAC-адрес можно подделать, но все-таки не стоит пренебрегать такой простой защитной мерой, которая без особых проблем реализуется на большинстве современных коммутаторов и, даже, концентраторов.

Узлы (в основном, шлюзы, диспетчеры и мониторы) должны быть настроены таким образом, чтобы блокировать все попытки несанкционированного доступа к ним. Для этого можно воспользоваться как встроенными в операционные системы возможностями, так и продуктами третьих фирм. А так как мы работаем в России, то я рекомендую применять средства, сертифицированные в Гостехкомиссии России, тем более что таких средств немало.

VLAN

Технология виртуальных локальных сетей (VLAN) обеспечивает безопасное разделение физической сети на несколько изолированных сегментов, функционирующих независимо друг от друга. В IP телефонии эта технология используется для отделения передачи голоса от передачи обычных данных (файлов, e-mail и т.д.). Диспетчеры, шлюзы и IP-телефоны помещают в выделенную VLAN для передачи голоса. Как я уже отметил выше, VLAN существенно усложняет жизнь злоумышленникам, но не снимает всех проблем с подслушиванием переговоров. Существуют методы, которые позволяют злоумышленникам перехватывать данные даже в коммутированной среде.

Шифрование

Шифрование должно использоваться не только между шлюзами, но и между IP-телефоном и шлюзом. Это позволит защитить весь путь, который проходят голосовые данные из одного конца в другой. Обеспечение конфиденциальности не только является неотъемлемой частью стандарта H.323, но и реализовано в оборудовании некоторых производителей. Однако этот механизм практически никогда не задействуется. Почему? Потому что качество передачи данных является первоочередной задачей, а непрерывное зашифрование/расшифрование потока голосовых данных требует времени и вносит зачастую неприемлемые задержки в процесс передачи и приема трафика (задержка в 200 ÷ 250 мсек может существенно снизить качество переговоров). Кроме того, как уже было сказано выше, отсутствие единого стандарта не позволяет принять всеми производителями единый алгоритм шифрования. Однако справедливости ради надо сказать, что сложности перехвата голосового трафика пока позволяют смотреть на его шифрование сквозь пальцы.

Кстати, если вы все-таки решитесь использовать шифрование, то помните, что, шифруя голосовые данные, вы скрываете их не только от злоумышленника, но и от средств обеспечения контроля качества (QoS), которые не смогут предоставить им соответствующую полосу пропускания и приоритетное обслуживание. Устранив одну проблему (беззащитность), перед вами встает другая (качество обслуживания). И можно быть уверенным, что при таком раскладе вы предпочтете решение второй проблемы, пренебрегая решением первой. Кстати, шифровать можно тоже не все подряд. Сигнальные протоколы, используемые в IP-телефонии, шифровать не рекомендуется, т.к. в этом случае вы зашифруете и всю служебную информацию, необходимую для поддержания работоспособности всей сети.

Но не стоит сразу отказываться от шифрования - все-таки обезопасить свои переговоры также необходимо. Поэтому стоит с умом подходить к шифрованию VoIP-данных. Например, компания Cisco рекомендует вместо туннеля GRE или применения VPN-концентраторов Cisco VPN 3000 использовать команду Crypto в операционной системе IOS своего оборудования, что позволяет защитить данные при сохранении качества обслуживания. Кроме того, можно использовать выборочное шифрование только для определенных полей в VoIP-пакетах.

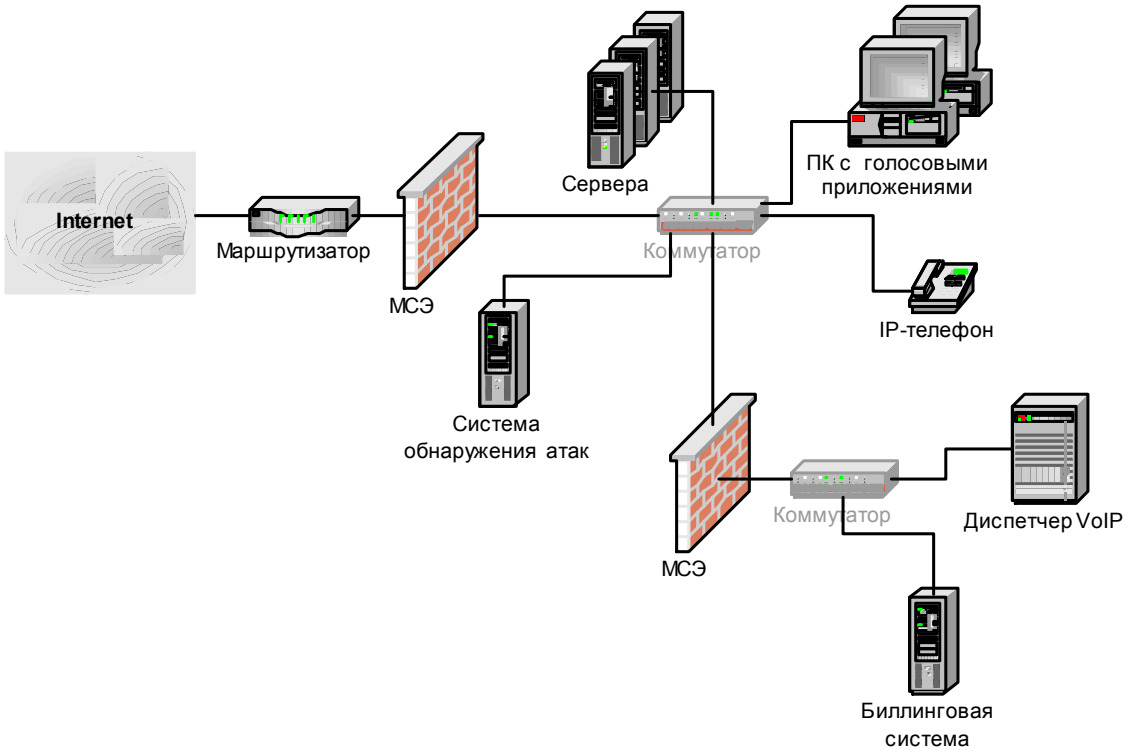

Рис.3.Фрагмент защищенной сети IP-телефонии

Межсетевой экран

Для защиты корпоративной сети обычно используется межсетевые экраны, которые с тем же успехом могут быть использованы и для защиты VoIP-инфраструктуры. Единственное, что необходимо сделать - добавить ряд правил, учитывающих топологию сети, местоположение установленных компонентов IP-телефонии и т.д. Например, доступ к Cisco CallManager из Internet или демилитаризованной зоны обычно блокируется, однако в случае использования Web-ориентированного управления такой доступ должен быть разрешен, но только для 80-го порта и только для ограниченного диапазона внешних адресов. А для защиты SQL-сервера, входящего в состав Cisco CallManager, можно запретить доступ со всех портов кроме 1433-го.

Кстати, существует два типа межсетевых экранов, которые могут быть использованы для защиты компонентов IP-телефонии. Первый из них, корпоративный, ставится на выходе из корпоративной сети и защищает сразу все ее ресурсы. Примером такого МСЭ является CiscoSecure PIX Firewall. Второй тип - персональный, защищающий только один конкретный узел, на котором может стоять абонентский пункт, шлюз или диспетчер. Примерами таких персональных МСЭ являются RealSecure Desktop Protector или BlackICE PC Protector. Кроме того, некоторые операционные системы (например, Linux или Windows 2000) имеют встроенные персональные межсетевые экраны, что позволяет задействовать их возможности для повышения защищенности инфраструктуры VoIP.

В зависимости от используемого стандарта IP-телефонии применение межсетевых экранов может повлечь за собой разные проблемы. Например, после того, как с помощью протокола SIP абонентские пункты обменялись информацией о параметрах соединения, все взаимодействие осуществляется через динамически выделенные порты с номерами больше 1023. В этом случае МСЭ заранее "не знает" о том, какой порт будет использован для обмена голосовыми данными и, как следствие, будет такой обмен блокировать. Поэтому межсетевой экран должен уметь анализировать SIP-пакеты с целью определения используемых для взаимодействия портов и динамически создавать или изменять свои правила. Аналогичное требование предъявляется и для других протоколов IP-телефонии.

Еще одна проблема связан с тем, что не все МСЭ умеют грамотно обрабатывать не только заголовок протокола IP-телефонии, но и его тело данных, т.к. зачастую важная информация находится внутри него. Например, информация об адресах абонентов в протоколе SIP находится именно в теле данных. Неумение межсетевого экрана "вникать в суть" может привести к невозможности обмена голосовыми данными через межсетевой экран или "открытии" в нем слишком большой дыры, которой могут воспользоваться злоумышленники.

Аутентификация

Различные IP-телефоны поддерживают механизмы аутентификации, которые позволяют воспользоваться его возможностями только после предъявления и проверки пароля или персонального номера PIN, разрешающего пользователю доступ к IP-телефону. Однако надо заметить, что данное решение не всегда удобно для конечного пользователя, особенно в условиях ежедневного использования IP-телефона. Возникает обычное противоречие "защищенность или удобство".

RFC 1918 и трансляция адресов

Не рекомендуется использовать для VoIP IP-адреса, доступные из Internet, - это существенно снижает общий уровень безопасность инфраструктуры. Поэтому при возможности используйте адреса, указанные в RFC 1918 (10.x.x.x, 192.168.x.x и т.д.) и немаршрутизируемые в Internet. Если это невозможно, то необходимо задействовать на межсетевом экране, защищающем вашу корпоративную сеть, механизм трансляции адресов (network address translation, NAT).

Системы обнаружения атак

Выше уже было рассказано о некоторых атаках, которые могут нарушить работоспособность VoIP-инфраструктуры. Для защиты от них можно использовать хорошо себя зарекомендовавшие и известные в России средства обнаружения атак (intrusion detection system), которые не только своевременно идентифицируют нападения, но и блокируют их, не давая нанести вред ресурсам корпоративной сети. Такие средства могут защищать как целые сетевые сегменты (например, RealSecure Network Sensor или Snort), так и отдельные узлы (например, CiscoSecure IDS Host Sensor или RealSecure Server Sensor).

Заключение

Разносторонность и объемность темы не позволяет подробно рассмотреть все аспекты обеспечения информационной безопасности IP-телефонии. Но те аспекты, которые мне удалось осветить и знания о которых вы можете расширить с помощью дополнительных ресурсов, все же показывают, что VoIP - не такая закрытая и непонятная область, как это кажется на первый взгляд. К ней могут быть применены уже известные по обычной телефонии и IP-сетям методы нападения. А относительная легкость их реализации ставит безопасность на первое место, наряду с обеспечением качества обслуживания IP-телефонии.

Дополнительные ресурсы

- Архитектура безопасности корпоративных сетей SAFE компании Cisco Systems - http://www.cisco.com/warp/public/779/largeent/issues/security/safe.html
- Архитектура SAFE для IP-телефонии: (SAFE: IP Telephony Security in Depth) - http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.htm
- Thomas, Michael. "SIP Security Framework" 12 July 2001 - http://search.ietf.org/internet-drafts/draft-thomas-sip-sec-framework-00.txt
- Liu, Jing. "The Security Architecture of H.323" - http://www.hut.fi/~yanli/Jing/home.html

Об авторе:

Алексей Викторович Лукацкий, заместитель директора по маркетингу Научно-инженерного предприятия "Информзащита" (Москва). Автор книг «Обнаружение атак» и «Атака из Internet». Сертифицированный инструктор по безопасности компании Internet Security Systems. Сертифицированный инженер по безопасности компании Check Point Software Technologies. Связаться с ним можно по тел. (095) 937-3385 или e-mail: luka@infosec.ru.

06 мая 2002 г.