
С IP-телефонией, как и любой новой технологией, связано множество различных мифов, слухов и домыслов, мешающих ее повсеместному распространению. Многие из них касаются безопасности IP-телефонии. Апологеты традиционной телефонии утверждают, что коль скоро в технологии VoIP в качестве среды передачи используется протокол IP, то к ней применимы и все сетевые атаки, а, следовательно, IP-среда для передачи голосового трафика не подходит. С одной стороны, они правы: атаки действительно возможны. Однако аналогичные атаки (прослушивание, фальсификация абонента и другие) применимы и к традиционной телефонии (см. врезку "Стоимость перехвата информации..."). Более того, в случае с традиционной телефонией реализовать эти атаки гораздо проще, а обнаружить и локализовать - намного сложнее. А по стоимости защиты обычные телефонные переговоры отличаются от более современной IP-телефонии на несколько порядков (в худшую сторону). Но, конечно же, чтобы новая технология позволила обмениваться звонками защищенным образом, ее не обходимо правильно внедрить и настроить.

**Разделение сети на сегменты**

Главное, что необходимо сделать при построении инфраструктуры IP-телефонии, - отделить ее от сегментов, в которых передаются обычные данные (файлы, электронная почта и т.д.). Это можно сделать как с помощью технологии виртуальных локальных сетей (VLAN), так и с помощью межсетевых экранов (МЭ). Первый вариант более эффективен и не требует никаких дополнительных инвестиций, так как механизм VLAN реализован в большинстве коммутаторов. Подобная сегментация позволит создать дополнительный рубеж, предупреждающий прослушивание переговоров обычными пользователями. Хорошей практикой является использование отдельного адресного пространства для сегментов IP-телефонии (например, из диапазонов, указанных в RFC 1918). Если сеть, передающая голос поверх протокола IP, имеет достаточно большие масштабы, то в ней не обойтись без динамической адресации по протоколу DHCP. В этом случае необходимо использовать два DHCP-сервера: один для голосовой сети, а второй для сети данных.

**Фильтрация и контроль доступа**

Голосовые шлюзы (Voice Gateway), подключенные к телефонной сети общего

пользования (ТфОП), должны отвергать все протоколы IP-телефонии (H.323, SIP и другие), приходящие из сегмента данных корпоративной сети. Зачастую поддержка протоколов IP-телефонии реализуется в маршрутизаторах с интеграцией сервисов (Integrated Services Router), что позволяет сэкономить на оборудовании, обеспечивая при этом поддержку самых современных технологий. В этом случае встроенный в маршрутизатор пакетный фильтр с контролем состояния может отслеживать любые нарушения в голосовом обмене и, например, блокировать пакеты, которые не являются частью процедуры установления вызова. Помимо встроенных в компоненты IP-телефонии механизмов фильтрации и контроля доступа существуют и специальные решения, защищающие элементы голосовой инфраструктуры от возможных несанкционированных воздействий. К таким решениям относятся межсетевые экраны (МЭ), шлюзы прикладного уровня (Application Layer Gateway, ALG) и специализированные пограничные контроллеры (Session Border Controller).

**Выбор межсетевого экрана**

Для защиты сети IP-телефонии подходит не всякий межсетевой экран - он должен удовлетворять ряду специфичных требований, присущих именно этой технологии передачи голоса. Например, протокол передачи голосовых данных RTP использует динамические UDP-порты, исчисляемые тысячами. Попытка разрешить их все на межсетевом экране приводит к открытию одной большой "дыры" в защите. Следовательно, межсетевой экран должен также динамически определять используемые для связи п орты, открывать их в начале телефонного разговора и закрывать по его окончании.

Вторая особенность заключается в том, что ряд протоколов, например SIP, помещает информацию об используемых параметрах соединения не в заголовок пакета, а в тело данных. Поэтому обычный пакетный фильтр, исследующий только адреса и порты получателя и отправителя, а также тип протокола, в данном случае будет абсолютно бесполезным. Межсетевой экран должен уметь анализировать не только заголовок, но и тело данных пакета, вычленяя из него всю необходимую для организации соединения информацию.

**Прикладные шлюзы и пограничные контроллеры**

Другая серьезная проблема, решение которой необходимо продумать до приобретения межсетевого экрана, - трансляция сетевых адресов (Network Address Translation, NAT). Коль скоро при установке вызова используются динамические порты, указанные в запросе на установление соединения между абонентами, то технология скрытия топологии сети путем трансляции адресов делает телефонные

переговоры невозможными. Решением проблемы является использование специальных прикладных шлюзов (ALG), выпускаемых в виде выделенных устройств или интегрированных в межсетевые экраны, "понимающие" протоколы с динамическими портами (например, SIP или RTCP). Некоторые производители выпускают только специализированные защитные шлюзы для обработки VoIP-трафика. Но при их выборе следует помнить, что в защите корпоративной сети все равно не обойтись без обычного МЭ, умеющего анализировать не только протоколы H.323, SIP и MGCP, но и другие распространенные в сетях протоколы: HTTP, FTP, SMTP, SQL*Net и т.д.
Ряд производителей предлагают решение проблемы защиты путем использования специализированных пограничных контроллеров (SBC). По сути, эти устройства во многом аналогичны описанным выше прикладным шлюзам.

**Защита от подмены**
Динамическая адресация во многих элементах инфраструктуры IP-телефонии дает злоумышленникам большой простор для деятельности: они могут "выдать" свой IP-адрес за IP-телефон, сервер управления звонками и т.д. А значит, перед администратором сети возникает задача аутентификации всех участников телефонных переговоров. Для этого необходимо использовать различные стандартизированные протоколы, включая 802.lx, RADIUS, сертификаты PKI X.509 и т.д. И, конечно, нельзя сбрасывать со счетов уже упомянутые выше правила контроля доступа на маршрутизаторах и МЭ, усложняющие злоумышленникам задачу подключения к голосовым сегментам.
Указанные методы позволяют эффективно бороться с "левыми" подключениями, в отличие от традиционной телефонии, где эта задача если и решается, то очень дорогостоящими средствами.

**Шифрование**
Шифрование - наиболее эффективный способ сохранить телефонные переговоры в тайне (см. врезку "Скремблеры и вокодеры..."). Однако такая функциональность влечет за собой ряд сложностей, которые необходимо обязательно учитывать при построении защищенной сети связи.

**Скремблеры и вокодеры для защиты традиционной телефонии**
Среди средств защиты особняком стоят вокодеры (voice coder) и скремблеры, которые осуществляют шифрование телефонных переговоров. Очевидно, что такие устройства должны быть установлены у всех участников защищенных переговоров. Механизм шифрования встраивается в телефон или поставляется в виде

отдельного устройства. В первом случае абонентский терминал становится слишком дорогим (и приходится отказываться от многофункциональных и удобных телефонных аппаратов зарубежного производства), во втором - практически полностью отсутствует возможность масштабирования, и пользование телефоном становится крайне неудобным. Оснастить каждого абонента скремблером или вокодером - задача не из легких. Если прибавить сюда цену телефонного аппарата и стоимость установки защитных устройств, получатся поистине астрономические цифры. Так что такой способ защиты традиционной телефонии нельзя считать экономичным.
Одна из самых главных проблем - задержка, добавляемая процессом зашифрования/расшифрования. В случае применения потокового шифрования задержка гораздо ниже, чем при использовании блочных шифров, но полностью от нее избавиться не удастся. Эта проблема решается путем использования более быстрых алгоритмов или включения механизмов QoS в модуль шифрования.
Еще одна трудность - накладные расходы, связанные с увеличением длины передаваемых пакетов. Для протокола IPSec размер добавляемого заголовка составляет около 40 байт, что достаточно много для 50-70-байтовых пакетов IP-телефонии. Впрочем, скорости современных сетей постоянно растут, и с течением времени эта проблема будет снята. А пока оптимальным решением обеих проблем является протокол SecureRTP (SRTP), принятый в качестве стандарта весной 2004г. (RFC 3711).

**Защита от нарушения работоспособности**
Несмотря на то что различные компоненты IP-телефонии потенциально подвержены атакам "отказ в обслуживании" (о сбоях в традиционной телефонии см. врезку "Перемаршрутизация звонков..."), существует целый ряд защитных мер , предотвращающих как сами DoS-атаки, так и их последствия. Для этого можно использовать встроенные в сетевое оборудование механизмы обеспечения информационной безопасности, а также дополнительные решения:
разделение корпоративной сети на непересекающиеся сегменты передачи голоса и данных, что предотвращает появление в "голосовом" участке распространенных атак, в том числе и DoS;
применение специальных правил контроля доступа на маршрутизаторах и МЭ, защищающих периметр корпоративной сети и отдельные ее сегменты;
использование системы предотвращения атак на сервере управления звонками и ПК с голосовыми приложениями;
установку специализированных систем защиты от DoS- и DDoS-атак;
«применение специальных настроек на сетевом оборудовании, которые

предотвращают подмену адреса, часто используемую при DoS-атаках, и ограничивают полосу пропускания, не позволяя вывести из строя атакуемые ресурсы большим потоком бесполезного трафика.

**Управление**

Для удаленного управления использование защищенных протоколов доступа (например, SSH) является обязательным (в данном случае шифрование вносит гораздо меньше задержек, чем при шифровании голосовых данных). Если же доступ к какому-либо компоненту сети IP-телефонии осуществляется по обычному протоколу (например, по HTTP), то непременным условием такого доступа должно быть применение протокола IPSec или SSL. В противном случае любой злоумышленник сможет не только перехватывать все данные с незащищенным элементом, но и подменять их.

Если требование криптографии вступает в конфликт с производительностью, то шифрованием на IP-телефонах или голосовых приложениях на ПК можно пренебречь. Если, конечно, к сети не применяются законодательные требования защиты всей конфиденциальной информации (включая и телефонные разговоры). При отказе от скрытия голосового трафика его необходимо в обязательном порядке отделить от всех остальных типов, передаваемых данных с помощью VLAN. При этом передача голоса между офисами должна быть защищена с помощью криптографических преобразований. Для этих целей можно задействовать встроенный в маршрутизаторы механизм IPSec VPN или установить отдельные шифраторы, сертифицированные в ФСБ России.

**Организационные вопросы**

Основная проблема безопасности IP-телефонии - не динамически открываемые порты на межсетевом экране, не NAT и не снижение качества голоса в результате шифрования. Все эти вопросы давно и эффективно решаются. Главная беда - "в головах", как говорил профессор Преображенский в "Собачьем сердце", а точнее, в недооценке существующих рисков и в непонимании новых технологий. Например, во многих организациях и компаниях существует классификатор конфиденциальной информации, обрабатываемой в автоматизированной системе. Но только в немногих организациях классифицируются еще и голосовые данные, передаваемые в рамках инфраструктуры IP-телефонии. А между тем информация, не включенная в такой классификатор, находится вне зоны внимания службы информационной безопасности и оказывается совершенно не защищенной.

**Заключение**

В опубликованном годовом отчете IBM "Security Threats and Attack Trends Report" приведен анализ основных угроз года прошедшего и дается прогноз на 2005 г. По мнению экспертов, IBM, увеличение числа сетей IP-телефонии приведет к росту угроз для их существования и бесперебойного функционирования. Поэтому обеспокоиться защитой внедряемой или уже внедренной инфраструктуры IP-телефонии необходимо именно сейчас, чтобы позже не "кусать себе локти". И это не так трудно, как кажется на первый взгляд. Существуют технологии, значительно повышающие защищенность VoIP, и они давно известны специалистам по информационной безопасности. Более того, эти технологии зачастую уже внедрены в компоненты, применяемые в построении среды передачи голоса поверх протокола IP. А значит, надо просто воспользоваться ими.