Эссе по курсу "Защита информации", кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ), http://www.re.mipt.ru/infsec
студента 113 гр. Тихонова Е.О.

Проблема безопасности IP-Телефонии.
(IP-phone security)

07.05.2005

Общая информация

Есть различные толкования самого названия «IP-телефония», верно передающие суть явления. Оно может расшифровываться как Интернет-телефон (Internet Phone) или как передача голоса поверх протокола IP (часто встречается обозначение VoIP - Voice-over-IP), который ранее использовался только для передачи данных, а не голосовой информации.

Идея заключается в преобразовании сигнала (голоса человека) в цифровой вид, сжатии. Затем - разбиение его на пакеты и пересылка через сеть, основанную на протоколе IP (Internet Protocol) в реальном времени (с использованием TCP/IP). Размеры пакетов должны быть не очень большими, чтобы собеседники вовремя получали их, и речь была непрерывной. На конечном пункте сигнал преобразуется обратно в аналоговую форму и может быть услышан собеседником. Весь процесс обычно занимает 200-400 мс. Абонентские пункты ("телефоны") могут быть реализованы и аппаратным и программным способом.

Посредник, который соединен с телефонной линией (от телефона, или, например, факса), а с другой стороны с IP-сетью называется шлюзом (gateway). На приемной стороне также расположено аналогичное устройство. Оно может выполнять и дополнительную обработку сигнала.

В распределенной сети IP-телефонии необходим также диспетчер, отвечающий за распределение вызовов между шлюзами (примером может служить Cisco CallManager). В его возможности может входить аутентификация и авторизация абонентов, ведение счета за услуги и владение данными о клиентах. Обычно такого диспетчера называют администратором. Управление счетом обычно осуществляется через web-интерфейс и это имеет свои последствия для безопасности.

Так как протокол IP не предназначен для передачи информации в реальном времени, могут иметь место пропадание пакетов (или приход их в неприемлемое время), различного рода задержки. Но если потеря одного пакета еще не слишком критична, то потеря нескольких может привести к большим неудобствам. Значительны и задержки в получении пакетов на удаленном шлюзе (например, в случае прихода пакетов в неправильном порядке).

В данное время основной недостаток IP-телефонии - низкое качество связи, связанное именно с этими проблемами, и, в отличие от традиционной телефонии, оно снижается при больших нагрузках в сети. Но технология является очень дешевой, в основном за счет повсеместного распространения Интернета (Internet).

Так как важно не только передать сообщение, но и воспроизвести его, то для VoIP крайне важно соблюдение одного и того же стандарта на передатчике и на приемнике. Некоторое время после появления технологии, компании, производящие оборудование и программное обеспечение вообще использовали закрытые протоколы: обе стороны должны были пользоваться услугами одной и той же фирмы. Позже Intel и Microsoft стали вести разработки программного обеспечения на основе стандарта H.323. Второй популярный современный стандарт - SIP протокол.

Типичные угрозы безопасности IP-Телефонии

Наибольшее распространение (в основном, за рубежом) IP-телефония получила в бизнесе и, кроме того, она осуществляется на основе доступной всем и хорошо известной сети, не требуя специальных аппаратных устройств. По этим причинам она часто подвергается различного рода атакам.

Большинство проблем, связанных с угрозами безопасности IP-телефонии, присущи и классической телефонии (или имеют в ней прямые аналоги).

- **Перехват данных (прослушивание):**

Прослушивание разговоров - нарушение конфиденциальности, самая частая проблема телефонии. Не нее обращается особое внимание, когда речь идет о переговорах или передачи имеющих большую ценность сведений. В то же время, осуществить ее легко, с помощью сниффера.

Казалось бы, все (или почти все) протоколы IP-T поддерживают шифрование, однако, задержки из-за этого вызывают большие неудобства (поэтому во всех программных и аппаратных продуктах по умолчанию шифрование отключено) и данные в большинстве случаев передаются в прямом виде.

Данные дампа, полученные с помощью слежения за трафиком легко можно конвертировать в звуковые. Например, для телефона CISCO со сжатием кодеком G.711, можно использовать утилиту vomit (Voice Over Misconfigured Internet Telephones).

Особенно критично это, в случае если злоумышленник может изменить маршруты движения трафика, став узлом, через который проходит интересующий его трафик. В Интернете это заметить крайне сложно, поэтому любой незашифрованный трафик должен считаться небезопасным.

- **Перехват соединения и имитация**

Злоумышленник может, как полностью перехватить соединение, выдавая себя за одну из сторон, так и вставлять в разговор свои отдельные пакеты (осуществлять имитацию). Например, добавлять слова, скомпилированные из предыдущих фраз или отдельных звуков. Но если перехват соединения иногда имеет место, то второе - очень затруднительно (время- и трудоемкая операция), в то время как разговор ведется в режиме реального времени.

- **Отказ в обслуживании (выведение из строя оборудования)**

В случае IP-телефонии отказ в обслуживании можно вызвать не только физическими воздействиями, но и осуществлением DoS-атаки (или распределенной версии, DDoS-атаки), весьма обычной для Интернета. Существует множество программ и способов сделать это (Land, Ping of Death, Smurf, UDP Flood).

Именно использование широко распространенных сетей делает эту атаку столь легко используемой против системы VoIP.

Если традиционная телефонная связь гарантирует качество в слабой зависимости от нагрузок, то IP-телефония крайне чувствительна к ним. При достаточно большом количестве "шумовых" пакетов, маршрутизаторы могут замедлить темп работы (и сделать невозможным общение), вследствие большой загруженности пакетами, так как потеря даже небольшого количества, сводит качество разговора на крайне низкое из-за искажения и пропадания части голосовых сообщений.

Возможным решением является резервирование полосы пропускания для IPT, например, с помощью протокола RSVP.

Но, как показала практика, это менее серьезная проблема, чем прослушивание. В течение трех дней проводилось тестирование фирмой Miercom, сотрудники которой после выяснения топологии IP-сети старались найти уязвимости и вызвать отказ в обслуживании оборудования системы Cisco CallManager. Удалось прослушать трафик (но он был зашифрован 128-битным

ключом, который за время теста расшифровать не удалось), то попытка DoS-атака успехом не увенчалась.

- **Подмена номера (выдача себя за другое лицо)**

В IP-телефонии роль телефонного номера выполняет IP-адрес. Существуют различные способы его подмены, которые могут привести к тому, что злоумышленник может быть принят за одну из сторон. Избежать этого можно с помощью аутентификации, что делается во всех VoIP-стандартах.

- **Атаки на абонентские пункты (удаленный доступ и пр.)**

Одним из существенных компонентов IP-телефонии является программное обеспечение, поэтому безопасность телефонии значительно зависит от уязвимостей в нем. Как в собственном, так и в операционной системе и стороннем ПО, установленном на компьютере (как правило, им является персональный компьютер). Обычно это - наименее защищенное устройство в цепи VoIP, так как в нем возможны атаки специфичные не только для IP-телефонии, например, различные вирусы, трояны.

Так, в ноябре 2004 из-за ошибки типа "переполнение кучи" в библиотеке MSASN1.DLL в функциях, отвечающих за безопасную передачу данных (использовалась для SSL в IIS, IP-телефонии и так далее) обнаружилась уязвимость, эксплуатировавшаяся в различных червях.

- **Вопросы конфиденциальности и атаки на диспетчеры**

Потенциальная угроза есть и по отношению к серверу диспетчера: образом, аналогичным и атаке на абонентский пункт может быть контроль получен над ним. Получение административного доступа к АТС (с системой счетов и информацией о клиентах) чревато получением конфиденциальных данных о клиентах, таких как информация о разговорах пользователей (имена абонентов, продолжительность и время разговора, причина конца вызова и т.п.), изменением их и удалением. В частности, причиной может быть желание аннулировать некоторые счета.

Остается и вопрос о доверии администрации, но его в большинстве случаев нельзя разрешить, так как у компании должна быть информация о клиентах, и она может быть использована не только в корпоративных целях, но и при злоупотреблениях служебными полномочиями. Выбор использования, например, система PIN-кодов зависит от политики диспетчера.

- **Кража сервисов (получение физического доступа к телефонному аппарату и использование чужих сервисов)**

Избежать можно ограничением только физического доступа и аккуратным отношением к конфиденциальности информации о номере, счете, пароле для входа в систему. По возможности следует все служебные аппараты разместить в специально оборудованных серверных комнатах.

- **Несанкционированное изменение конфигурации**

Вопрос из области защиты программного обеспечения, который не входит в компетенцию данного эссе.

- **Мошенничество со счетом**

Соблазнительным является в случае IP-телефонии совершать бесплатные звонки. Это может быть осуществлено в первую очередь за счет различных махинаций со счетом (например, после успешно совершенной атаки на диспетчера).

Но возможны и другие случаи. Например, в системе Tario несколько первых месяцев была ошибка в программном обеспечении и на сервере администрации и на компьютере пользователя. Счет заводился после введения PIN-кода с карточки, и конечного пользователя

определить было невозможно. Даже когда счет был исчерпан, звонок и даже сессия не прекращались, и можно было говорить и звонить "в кредит". Который никто не оплачивал, предпочитая завести новый счет.

- **Совмещенность линии управления и линии передачи данных**

И служебная информация о соединении и речевой поток в отличие от обычной телефонии передается в рамках одной и той же сети. Если злоумышленник имеет доступ к сигнальной информации и речевым пакетам (что в данном случае - аналогичные действия), злоумышленник может выполнить и переадресацию вызова и имитацию по отношению к одной или даже двум сторонам. Возможны также инициированные им конец вызова и так далее.

- **Большое количество стандартов**

В ряде случаев может использоваться не один ид двух-трех популярных протоколов, а менее известный (например, по экономическим причинам),в котором можгут быть обнаружены уязвимости.

Однако, в апреле текущего года, рядом компаний (консорциум VoIP Security Alliance: McAfee, MCI, PricewaterhouseCoopers, Samsung Telecommunications America, Sprint, VeriSign и др.) был создан комитет, задачами которого объявлены определение требований к безопасности IP-телефонии и выработке единых стандартов служб, систем управления, аутентификации, поиску уязвимостей и механизмов потенциальных атак.

Средства защиты IP-телефонии

Кроме вышеуказанных средств противодействия некоторым угрозам, можно выделить относящиеся сразу к нескольким областям, комплексным методам. Они же могут служить рекомендациями при построении IPT системы.

- Ограничение доступа к оборудованию и своевременное аннулирование обнаруженных уязвимостей (как в программном обеспечении IP-телефонии, так и в ОС).

- Следует периодически проверять сеть на наличие несанкционированно подключенных устройств, подключенных к сетевому кабелю.

Для этого существуют специальные сканеры (Internet Scanner, Nessus), удаленно распознающих наличие в сети неизвестных устройств. Они могут защищать как сетевые сегменты (RealSecure Network Sensor, Snort), так и отдельные узлы (CiscoSecure IDS Host Sensor, RealSecure Server Sensor).

- Контроль доступа по MAC-адресу (соответствие IP-адрес - MAC-адрес)

MAC-адрес можно изменить и подделать, но даже эта нехитрая защита (легко реализуемая в сетевом оборудовании) в ряде случаев может дать результат и затруднить задачу злоумышленнику.

- Организация и вынос IP-телефонии в частные виртуальные сетеи (VLAN).

Это позволит разграничить сетевое пространство передачи "обычных" данных и VoIP. Так, серверы IP-телефонной инфраструктуры логично разместить в отдельном сетевом сегменте, защищенном средствами защиты коммутатора и маршрутизатора (списками контроля доступа, системами обнаружения атак и так далее) и специализированными пакетами (такими, как межсетевые экраны, системы аутентификации).

- Шифрование важных разговоров

Правда, сразу же увеличатся временные задержки, уменьшая качество разговоров, но эта возможность должна быть предусмотрена.

- Использование межсетевых экранов

Их следует устанавливать как на выходе корпоративной сети (если IP-телефонная система предназначена для использования в фирме, в случае частного абонента этот этап защиты не будет актуален), так и экраны, защищающие конкретный узел (шлюз, диспетчер, абонентский пункт). Могут быть использованы и встроенные в ОС межсетевые узлы (они есть в Linux и Windows 2000, Windows 2003).

Однако, в ряде случаев с применением МСЭ следует быть осторожным. Так, при использовании SIP номера портов, через которые происходит взаимодействие, происходит динамически, при каждом соединении, следовательно, применяемый МСЭ должен уметь анализировать SIP-пакеты для определения, какие порты ему не следует блокировать и уметь динамически же менять собственные правила.

- Использование аутентификация (пароль или PIN-код для доступа к службам)

Все IP-телефоны поддерживают механизмы аутентификации, гарантирующие правомерность обращения к функциям IP-телефонии. Правда, это лишние затруднения для конечного пользователя, особенно при регулярном использовании VoIP.

- Использование в корпорационной IP-системе адресов, являющихся адресами виртуальных сетей, в соответствии с RFC 1918: 10.x.x.x, 192.168.x.x и 172.16-31.x.x

- Смена и установка устойчивых паролей на доступ к системе администрации через Web-интерфейс

Во многих случаях это может быть особо уязвимый узел системы, особенно при доступе через HTTP, где пароли передаются прямым текстом. Целесообразнее - использовать и более устойчивые системы администрирования.

Протокол H.323

Самый, пожалуй, популярный в VoIP стандарт - H.323, рекомендованный International Telecommunications Union (ITU).

В нем сформулированы общие требования к передаче чувствительного к скорости трафика (видео, аудио, голос) по сетям с негарантированным качеством услуг, например, Ethernet и IP, правила получения приоритета в глобальных и локальных сетях. Он состоит из рекомендаций по необходимому качеству, контролю вызовов, контролю доступа, управлению пропускной способностью шлюзов и узлов абонента, стандарты звуковых и видео кодер-декодеров.

Это протокол, образованный как компиляция уже существующих, поэтому обладающий общностью, но при этом весьма сложный. Он позволяет построить VoIP-систему от начала до конца.

Он включает в себя ряд предшествующих рекомендаций, среди которых H.323, H.324, H.235, которые напрямую относятся к безопасности.

H.235

H.235 реализует аутентификацию, контроль целостности, конфиденциальности и невозможность отказа от сообщений для голосовых данных.

Аутентификация может быть реализована с помощью алгоритмов симметричной криптографии (это не требует предварительного обмена информацией взаимодействующих устройств и меньше нагрузка на диспетчера), с использованием сертификатов или паролей или аутентификации IPSec.

Установка соединения происходит через 1300 TCP, через ненадежные каналы и возможны задержки, повторные передачи, потери.

H.233

Стандарт шифрования данных мультимедийной информации реального времени. Описание не включает в себя конкретных алгоритмов, ограничиваясь общими замечаниями.

H.234

Определяет, каким образом создаются ключи аутентификации. При этом могут быть использованы криптографические алгоритмы ISO 8732, Диффи-Хеллмана (Diffie-Hellman), RSA.

Протокол SIP (Session Initiation Protocol)

Стандарт SIP, созданный Internet Engineering Task Force, значительно проще H.323. Для него требуется вдвое меньшее количество служебных сообщений, при этом экономится значительное время, что критично в случае разговора реального времени. Протокол был создан на базе HTTP и SMTP. Взаимодействие происходит аналогичным образом по типу запрос-ответ (request - reply), все сообщения - текстовые, коды возврата такие же, как и в HTTP (например, 404 - абонент не найден, 200 - OK).

Он тоже не был создан специально для передачи голосовых данных, но его преимущества позволяют его использовать в этой области (хотя он используется и для игр). Тип передаваемых данных определяется протоколом описания сеанса SDP (Session Description Protocol). Тип данных может быть изменен динамически: например, во время разговора можно передать собеседнику изображение (фотографию) или текстовый документ. Может быть осуществлен даже переход на другой терминал (например, с мобильного телефона на компьютер).

Особыми мерами защиты SIP не обладает, и их нужно предусматривать самостоятельно.

Механизм аутентификации SIP регламентирован в RFC 2543, где предлагается использовать один из вариантов: базовую аутентификацию (как в HTTP), аутентификацию на базе PGP.

Дополнительными рекомендациями является описание стандарта IETF "SIP security framework" (Майкла Томаса), где описаны угрозы и методы защиты от них (например, защита на транспортном уровне с помощью TLS или IPSec).

Но, тем не менее, было обнаружено несколько уязвимостей при реализации ПО на основе протокола SIP. Так, в продуктах Cisco Systems были обнаружены ошибки, которые могут быть использованы для получения "привилегированного доступа или организации атак типа DoS, или вызвать нестабильное поведение системы". Объявлено, что "дыры пока никто не использовал, и они являются экзотическими"

Протокол MGCP

Протокол описан в рекомендациях RFC 2705. Вопросы безопасности рассматриваются в разделе Security.

Стандарт менее распространен, чем предыдущие, и применяется лишь в шлюзах. Последние могут работать с конечными устройствами, поддерживающими более популярные H.323, и SIP.

В MGCP при защите данных используется обычно ESP-протокол (спецификация IPSec).

Наряду с ним может быть применен и протокол AH (в сетях IPv4), обеспечивающий аутентификацию, целостность данных, защиту от повторений передаваемой информации, но не гарантирующий сохранения конфиденциальности данных.

Выводы

Возможности IP-телефонии очень разнообразны, и, вероятно, данная технология будет в будущем развиваться и широко применяться.

Однако весьма большое внимание следует уделять обеспечению безопасности: ip-телефония подвержена разнообразным атакам, как свойственным классической телефонии, так и являющимся уникальным для нее.

В текущее время сделано многое в этой области, но зачастую мешает отсутствие общих стандартов и технические трудности (например, шифрование – «времяемкая» операция, ухудшающая свойства связи в реальном времени).

Ссылки, использованные в работе:

http://www.discom.net.ru/docs/IP-secure.doc - Анализ угроз традиционной и IP телефонии

http://www.voipsa.org/ - Организация, с 29.03.2005 занимающаяся стандартизацией VoIP

http://citforum.ncstu.ru/security/articles/inform/ - статья «IP-опасность для бизнеса», Алексей Лукацкий, 2004 год

http://www.sipforum.org/ - Стандарты SIP

http://h323.com.ru - Стандарты H.323

http://cdo.bseu.by/library/ibs1/applic_l/video/h323/h323_rus.html - Стандарты H.323

Иллюстрации взяты из новостей:

http://stra.teg.ru/lenta/security/970 - (3 марта 2003)

http://www.cnews.ru/newsline/index.shtml?2003/03/03/141489 - (3 марта 2003)

http://www.megalib.com/books/678/012/1.htm - Хакер, номер #048, стр. 048-012-1