IP-ТЕЛЕФОНИЯ: УГРОЗЫ, АТАКИ И СПОСОБЫ ИХ ОТРАЖЕНИЯ

ВОЗМОЖНЫЕ УГРОЗЫ

- перехват данных;
- 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, так как злоумышленнику уже не нужен физический доступ к телефонной линии. Ситуацию ухудшает и то, что множество протоколов, построенных на базе стека TCP/IP, передают данные в открытом виде. Таким грехом страдают HTTP, SMTP, IMAP, FTP, Telnet, SQL*net, в том числе протоколы IP-телефонии. Перехватив голосовой IP-трафик (а он по умолчанию между шлюзами не шифруется), злоумышленник 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, который можно прослушать на любом компьютерном плейере. Эта утилита позволяет конвертировать голосовые данные, переданные посредством IP-телефонов Cisco и сжатые с помощью кодека G.711.

Перехват данных возможен как изнутри корпоративной сети, так и снаружи. Причем если во внутренней сети несанкционированно подключенное устройство, перехватывающее голосовые данные, с определенной долей вероятности будет обнаружено, то во внешней сети заметить 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 для IP-телефонии совсем не аксиома. Высокая нагрузка на сеть передачи оцифрованных голосовых данных приводит к существенному искажению и даже пропаданию части сообщений. Поэтому одна из атак на IP-телефонию может заключаться в посылке на сервер IP-телефонии большого числа "шумовых" пакетов.

Что характерно, для реализации атаки "отказ в обслуживании" - достаточно использовать широкие известные DoS-атаки Land, Ping of Death, Smurf, UDP Flood и т. д. Одно из решений - резервирование полосы пропускания с помощью современных протоколов, например RSVP.

Подмена номера

Для связи с абонентом в обычной телефонной сети необходимо знать его номер, а в IP-телефонии роль телефонного номера выполняет IP-адрес. Следовательно, возможна ситуация, когда злоумышленник, используя подмену адреса, выдает себя за нужного вам абонента. Именно поэтому задаче обеспечения аутентификации уделяется внимание во всех VoIP-стандартах.

Атаки на абонентские пункты

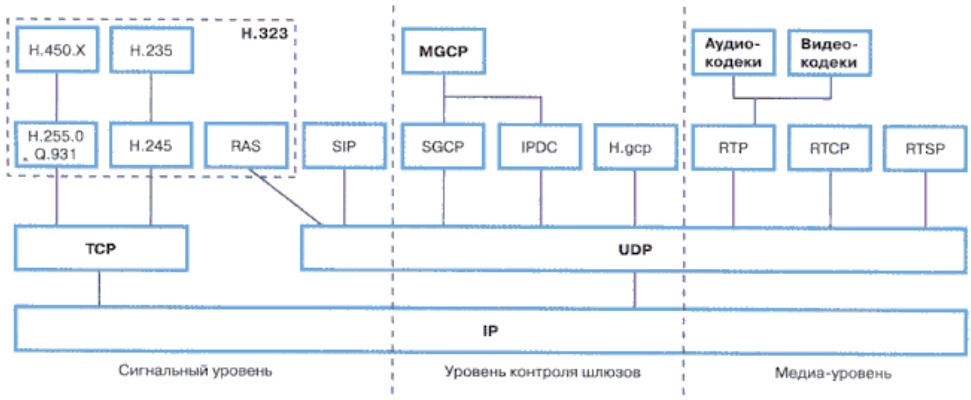
Абонентские пункты, реализованные на базе персонального компьютера, менее защищены, чем специальные IP-телефоны. Это относится и к любым другим компонентам IP-телефонии на программной основе и связано с тем, что на такие компоненты можно реализовать не только специфичные для IP-телефонии атаки. Сам компьютер и его составляющие (операционная система, прикладные программы, базы данных и т. д.) подвержены различным атакам, которые могут повлиять и на компоненты IP-телефонии.

Атаки на диспетчеров

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.), как для 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 клиентам, что нанесет ущерб всей инфраструктуре IP-телефонии, нарушив ее функционирование.

Стандарты IP-телефонии и механизмы их безопасности

Отсутствие единых принятых стандартов в данной области (рис. 1) не позволяет разработать универсальные рекомендации по защите устройств IP-телефонии. Каждая рабочая группа или производитель по-своему решает задачи обеспечения безопасности шлюзов и диспетчеров, тщательно их изучая, прежде чем выбрать адекватные меры по защите.



Архитектура протоколов IP-телефонии

Рис. 1. Архитектура протоколов IP-телефонии

Безопасность H.323

Протокол H.323 позволяет построить VoIP-систему от начала и до конца. Он включает в себя ряд спецификаций, в том числе 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 осуществляется как с помощью алгоритмов симметричной криптографии, так и с помощью сертификатов или паролей. Кроме того, спецификация H.235 позволяет использовать в качестве механизма аутентификации IPSec, рекомендуемый к применению и в других стандартах IP-телефонии.

После установки защищенного соединения 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 (необязательно телефонного, но и, скажем, для игр), не обладает серьезной защитой. Пытаясь усилить защищенность данного протокола, Майкл Томас из компании Cisco Systems разработал проект стандарта IETF, названный "SIP security framework", с описанием внешних и внутренних угроз для протокола SIP и способов защиты от них. К таким способам можно отнести защиту на транспортном уровне с помощью TLS или IPSec.

Безопасность MGCP

Стандарт MGCP может работать как с компонентами, поддерживающими H.323, так и с компонентами, поддерживающими SIP, использует для защиты голосовых данных протокол ESP и AH спецификации IPSec.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

Обеспечение безопасности выше приведенных протоколов рассмотрим на примере IPSec.

Архитектура IP Security (IPSec)

IPSec - это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов.

Гарантии целостности и конфиденциальности данных в спецификации IPsec обеспечиваются за счет использования механизмов аутентификации и шифрования соответственно. Последние, в свою очередь, основаны на предварительном согласовании сторонами информационного обмена т.е. "контекста безопасности" – применяемых криптографических алгоритмов, алгоритмов управления ключевой информацией и их параметров. Спецификация IPsec предусматривает возможность поддержки сторонами информационного обмена различных протоколов и параметров аутентификации и шифрования пакетов данных, а также различных схем распределения ключей. При этом результатом согласования контекста безопасности является установление индекса параметров безопасности (SPI), представляющего собой указатель на определенный элемент внутренней структуры стороны информационного обмена, описывающей возможные наборы параметров безопасности.
По сути, IPSec работает на третьем уровне, т. е. на сетевом уровне. В результате передаваемые IP-пакеты будут защищены прозрачным для сетевых приложений и инфраструктуры образом. В отличие от SSL (Secure Socket Layer), который работает на четвертом (т. е. транспортном) уровне и теснее связан с более высокими уровнями модели OSI, IPSec призван обеспечить низкоуровневую защиту.

Заголовок AH

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

Формат AH достаточно прост и состоит из 96-битового заголовка и данных переменной длины, состоящих из 32-битовых слов. Названия полей достаточно ясно отражают их содержимое: Next Header указывает на следующий заголовок, Payload Len представляет длину пакета, SPI является указателем на контекст безопасности и Sequence Number Field содержит последовательный номер пакета.

Следующий заголовок	Длина нагрузки	Зарезервировано
Индекс параметров безопасности		
Поле последовательного номера		
Данные аутентификации (переменной длины)		

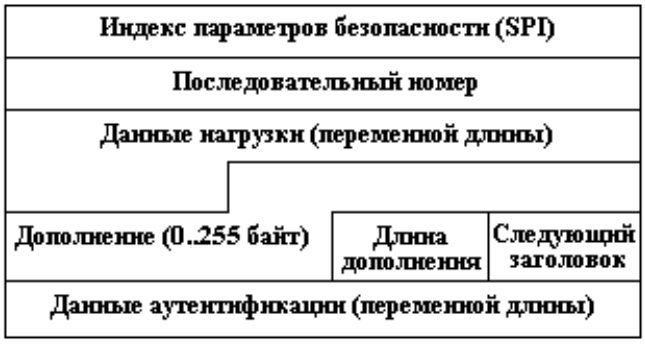
Формат заголовка AH.

Последовательный номер пакета был введен в AH в 1997 году в ходе процесса пересмотра спецификации IPsec. Значение этого поля формируется отправителем и служит для защиты от атак, связанных с повторным использованием данных процесса аутентификации. Поскольку сеть Интернет не гарантирует порядок доставки пакетов, получатель должен хранить информацию о максимальном последовательном номере пакета, прошедшего успешную аутентификацию, и о получении некоторого числа пакетов, содержащих предыдущие последовательные номера (обычно это число равно 64).
В отличие от алгоритмов вычисления контрольной суммы, применяемых в протоколах передачи информации по коммутируемым линиям связи или по каналам локальных сетей и ориентированных на исправление случайных ошибок среды передачи, механизмы обеспечения целостности данных в открытых телекоммуникационных сетях должны иметь средства защиты от внесения целенаправленных изменений. Одним из таких механизмов является специальное применение алгоритма MD5 (Message Digest 5): в процессе формирования AH последовательно вычисляется хэш-функция от объединения самого пакета и некоторого предварительно согласованного ключа, а затем от объединения полученного результата и преобразованного ключа.

Заголовок Encapsulated Security Payload (ESP)

В случае использования инкапсуляции зашифрованных данных заголовок ESP является последним в ряду опциональных заголовков, "видимых" в пакете. Поскольку основной целью ESP является обеспечение конфиденциальности данных, разные виды информации могут требовать применения существенно различных алгоритмов шифрования. Следовательно, формат ESP может претерпевать значительные изменения в зависимости от

используемых криптографических алгоритмов. Тем не менее, можно выделить следующие обязательные поля: SPI, указывающее на контекст безопасности и Sequence Number Field, содержащее последовательный номер пакета. Поле "ESP Authentication Data" (контрольная сумма), не является обязательным в заголовке ESP. Получатель пакета ESP расшифровывает ESP заголовок и использует параметры и данные применяемого алгоритма шифрования для декодирования информации транспортного уровня.



Формат заголовка ESP

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

Транспортный режим

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

Туннельный режим

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

расшифровки межсетевым экраном начального заголовка сетевого уровня пакет направляется получателю.

Internet Key Exchange (IKE)

IKE – протокол обмена ключами. IKE поддерживает набор различных примитивных функций для использования в протоколах. Среди них можно выделить хэш-функцию и псевдослучайную функцию.

Протоколы IKE решают три задачи: согласовывают алгоритмы шифрования и характеристики ключей, которые будут использоваться в защищенном сеансе; обеспечивают непосредственный обмен ключами (в том числе возможность их частой смены); наконец, контролируют выполнение всех достигнутых соглашений.

Заключение

Разносторонность и обширность темы не позволяют подробно рассмотреть обеспечение информационной безопасности IP-телефонии. Рассмотренный протокол IPSec - один из наиболее используемых и защищенных, поэтому я остановил свое внимание на нем. Однако, следует добавить следующие общие замечания:

1) 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.

2) 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 мс может существенно снизить качество переговоров).

3) как уже было сказано выше, отсутствие единого стандарта не позволяет принять всеми производителями единый алгоритм шифрования.

Литература, использованная для создания эссе:

1) http://osp.admin.tomsk.ru/lan/2001/04/020.htm - Дифференцированная защита трафика средствами IPSec.

2) http://www.datatelecom.ru/Reshen/Resh_bezop.htm - Шифрация на сетевом уровне по протоколу IPSec.

Дополнительная информация:

1) http://www.zeiss.net.ru/docs/cti/ip-tel3/ipteleph-3.htm -Что такое IP-телефония?

2) http://h323.com.ru - Стандарты H.323

3) http://www.ccc.ru/magazine/depot/96_07/print.html?0202.htm - RSVP — гарантия качества обслуживания в сетях TCP/IP

4) http://sure.org.ru/docs/networks/protocols/net_l/tcp_ip/net/rtp.htm - RTP - Протокол передачи видео- и аудиоинформации в реальном масштабе времени.

5) http://www.arcon.ru/about_ip.htm – Описание технологии VoIP.