БЕЗОПАСНОСТЬ VoIP-соединений

Б.Бахметьев, технический директор ЗАО "МТР-Связь"

Внедрение технологий пакетной коммутации идет семимильными шагами. Традиционные TDM-технологии стремительно вытесняются технологиями VoIP. Казалось, основная цель достигнута, себестоимость звонков снижена, инфраструктура сети оператора оптимизирована, можно только радоваться и пожинать плоды. На этом пути, как это бывает у всех первопроходцев, возникают разного рода препятствия. Как их преодолеть и на что обратить внимание?

Еще 20 лет назад технологии цифровых АТС казались связистам манной, неожиданно свалившейся с небес. После неуклюжих квазиэлектронных "Квантов" с не вполне дружественным интерфейсом (снабженным лишь матричным принтером и ассемблероподобным MML-языком), которые в советские времена все же казались прогрессивными и современными, связисты вдруг получили в свои руки действительно современные и мощные 5ESS, AXE и прочие "хайкомы" с "тадиранами". Слова ISDN, PRI и DSL деловито витали в воздухе во время любых разговоров на телекоммуникационную тематику. Перспективы были радужными, энтузиазм зашкаливал, все были заражены идеей тотальной замены давно и безнадежно одряхлевшего парка старых АТС. Автор застал даже не декадную, а еще машинную АТС и даже успел поработать с ее линиями. Части этой АТС благодарные шведы потом благоговейно забрали на ее историческую родину в музей, а сама АТС вошла в книгу рекордов Гиннеса. Ее многочисленных декадно-шаговых и координатных потомков ждала менее почетная судьба, и они бесславно сгинули на свалках. Чтобы был понятен контраст перехода, могу сказать, что практически во время последних дней работы машинной АТС автор в то же время принимал самое непосредственное участие во включении чуть ли не самого первого стыка МГТС с сигнализацией EDSS-1. Все дышало новизной, и казалось, что вектор развития телекоммуникаций задан если уж не на столетия, то на десятилетия точно.

Примерно в то же время в стране все большую популярность приобретал еще один неведомый и загадочный зверь – Интернет. Свалка картинок, чатов и инфодосок жила и развивалась своей параллельной жизнью. Технологии цифровой ISDN-телефонии (Integrated Services Digital Network) и Интернета, уже ставшие тогда привычными, казались такими далекими друг от друга и такими непохожими, что только самые смелые предрекали скорое их скрещивание. Но время осуществления предсказаний подкралось тихо и незаметно. Первые голосовые чаты в локальных сетях казались скорее забавой, чем реальной альтернативой телефону, для многих скайп был некой игрушкой. Возможность говорить, а не просто переписываться через компьютер многим казалась чем-то искусственным. Сама идея передачи голоса через Интернет вызывала четкий диссонанс в сознании, ведь основной потребитель телефонии не слишком силен в настройке компьютеров, да и процесс установления соединения казался настолько громоздким, что, казалось, вряд ли приживется в массовом сознании. Первый принятый в 1996 году международный протокол передачи данных через пакетную коммутацию получил свой идентификатор H.323 и поначалу выглядел экзотикой, предназначенный на долгую перспективу. Новое направление назвали короткой аббревиатурой VoIP (Voice over

IP – Голос поверх IP). Протокол H.323 был компромиссом между VoIP и традиционной технологией TDM (Time Division Multiplexing), унаследовав многие черты консервативной телефонии. Однако он сделал главное: показал, что VoIP будет внедряться незаметно для массового потребителя. Для него как раз ничего и не меняется, телефон на самом деле никто не собирался менять на громоздкий и сложный компьютер, вся тяжесть перехода ложилась на замученных связистов. И вот появились первые промышленные АТС с пакетными интерфейсами, первые софтсвичи и медиашлюзы, был разработан куда более гибкий протокол SIP. Качество все еще было ужасным, сама идея негарантированной доставки пакетов и "склеивания" их потом в стройную шеренгу таила в себе много проблем и недостатков, связанных с качеством передачи голоса. Но кроме "квакания" и раздражающего эха в трубке пионеры новых технологий столкнулись еще с одной бедой. Неожиданно операторы при расчете в биллинговых системах вдруг находили сумасшедшие счета с непонятными номерами и заоблачными цифрами в колонке "Итого". Если номер был все же более-менее опознаваем, абонент, получив счет, хватался за сердце и, выпив корвалола, божился, что не мог наговорить с Кот-д'Ивуаром на три тысячи долларов. Нет у него там родственников, он вообще впервые слышит название этой страны и плохо представляет, в какой части света она находится.

И вот тут связисты поняли, что попытка совместить строгую телефонию, где каждый шаг фиксируется и протоколируется, с абсолютно неконтролируемым Интернетом может закончиться весьма ощутимыми потерями финансов и своего реноме. Хорошо, если у вас изолированная корпоративная сеть, замкнутая сама на себя и не требующая выхода в публичную сеть, и вы закрыты от внешнего мира в своей внутренней сети, как Северная Корея. Но такая ситуация – лишь редкое исключение. Абсолютной изолированностью сейчас не могут похвастаться даже самые секретные сети, недаром в СМИ иногда всплывают сообщения о том, как какой-то хакер "взломал Пентагон". Очень забавно наблюдать, как в голливудском кинофильме подросток с дешевого телефона за 20 секунд, нажав пару кнопок, получает доступ к суперсекретному пульту запуска баллистической ракеты. Реалии суровой действительности не так сказочны, как это показано в кино, и чтобы получить доступ к хоть как-то защищенной сети, нужно приложить немало усилий. Однако, несмотря на всю сложность, вероятность вскрытия все же есть. Изначально VoIP замышлялся с одной самой главной мыслью: коль скоро пакетная коммутация и Интернет развиваются так стремительно и с такими головокружительными перспективами, то проще "смешать пакет и голос в одном флаконе" и тем самым сократить общие финансовые затраты. Расходы на инфраструктуру сразу резко сокращаются. Голос, по сути, – один из видов передаваемой информации, и нет экономического смысла выделять его в особый сервис со своей выделенной сетью. Здесь, как всегда, главной движущей силой выступили прежде всего деньги. Ради прибыли операторы готовы были пойти на все: и на плохое качество, и на смену или переобучение персонала, и на снижение безопасности – на любые жертвы ради снижения себестоимости. Итак, неизбежность решения вопросов безопасности VoIP стала окончательной и бесповоротной, и оставалось уделить ей максимальное внимание.

На самом деле безопасность VoIP не ограничивается лишь взломом учетной записи регистрации для последующих пиратских звонков. Учетная запись, или, по-другому, аккаунт, нужна серверу для опознавания и идентификации абонента. В отличие от традиционной телефонии, у аппарата уже нет привычного провода или выделенного временного тайм-слота. Опознавание идет на уровне простого логина и пароля, и если злоумышленник правильно указал пароль, то он получит полные права абонента, в том числе право звонить. Самый частый вид взлома тот, который дает максимальную финансовую выгоду взломщикам. Они, как и операторы и просто обыватели, любят прибыль. Для этого нужно получить тот самый аккаунт от SIP-АТС или АТА-адаптера, преобразующего IP-сеть в стандартный телефонный провод, и использовать его в качестве шлюза выхода в сеть общего пользования. По сути, получив пароль аккаунта, вы получаете ключ к деньгам. В обычной TDM АТС терминация трафика четко прописана по выделенным каналам с заранее обозначенными масками и форматами набора, и вклиниться наружу транзитом можно было разве только что через так называемую DISA (Direct Invard System Access – прямой внутренний доступ к системе), которая в России, кстати, так и не прижилась. DISA предназначалась для донабора внутреннего абонента АТС в целях экономии на секретаре и публичных телефонных номерах. Однако нерадивые администраторы оставляли возможность набирать через

DISA и междугородние номера, и вдобавок оставляли заводской гостевой пароль, чаще всего 1111. Злоумышленники, в то время чаще всего вьетнамские умельцы из общежитий гастарбайтеров, с успехом этим пользовались, звоня на АТС и донабирая с АТС куда угодно без всяких ограничений. Однако такие случаи не носили массового характера, они были единичны, и если пираты и получали редкий доступ к открытой DISA, то пользовались ею с максимальной загрузкой.

VoIP дает благодатное непаханое поле для терминации трафика в любую точку мира. Надо лишь, сохраняя честное выражение лица, на время стать абонентом SIP-сервера, сказав при регистрации заветный логин и пароль, и можно звонить куда хочешь и сколько хочешь, пока сторож, т.е. в нашем случае оператор, смотрит в другую сторону и ничего не подозревает. Взломщики, естественно, пользуясь открывшейся перспективой, льют трафик на самые дорогие направления, как правило, острова Океании, Кубу или другую экзотику. Механизм очень прост. Подбирается пароль к ATA-адаптеру или непосредственно к самому SIP-серверу, или взламывается операционная система, где стоит софтсвич, например любимый всеми Asterisk. Чаще всего оператор не привязывает аккаунт к IP- или MAC-адресу или, того хуже, оставляет открытым гостевой аккаунт. Как только пароль подобран, широкие ворота открыты. Самой большой проблемой теперь уже будет найти достаточное число абонентов, звонящих на эти самые дорогие зоны, и направлять звонки через Интернет на взломанный сервер, то есть абсолютно бесплатно. С местного абонента берется плата за звонок куда-нибудь в Науру, но при этом сам оператор никому за этот звонок не платит, а вся прибыль остается у взломщиков в кармане. В обычном варианте львиная доля дохода уходит международному оператору и норма прибыли совсем не так высока. В случае взлома SIP-АТС прибыль оператора равна доходу, т.е. вырастает в разы, все деньги от абонента остаются у злоумышленника. Обычно этим занимаются мелкие операторы из Юго-Восточной Азии, они не брезгуют ничем ради лишней прибыли. Крупный оператор не будет портить свое реноме на рынке. Но даже абонентов мелкого оператора хватит на то, чтобы нанести существенный финансовый урон. Как правило, они выбирают ночные часы, когда дежурная смена не очень внимательна и не успевает быстро отреагировать – зачастую это вообще не входит в ее компетенцию. За ночь при хорошем уровне трафика с одного ATA-адаптера нерадивого оператора, особенно если аккаунт позволяет совершать многоканальные звонки, можно наказать на десятки тысяч долларов. Пока утром придут ответственные за тарификацию, пока среагируют, будет уже поздно. Повторюсь: этот вид взлома – наиболее распространенный и, к сожалению, наиболее болезненный для коммерческих операторов, так как бьет по самому больному – по карману. По традиции, мы начинаем креститься, только когда молния уже ударила. Как же защититься от взлома?

Раньше, во времена аналоговой и TDM-телефонии, взламывать сеть можно было разве что с кросса или, как уже упоминалось выше, через DISA. Влезть в выделенный канал куда-нибудь в SDH (Synchronous Digital Hierarchy) практически нереально, так как в традиционных TDM-системах каждый бит информации строго учтен и расписан, любой чужак будет или гневно и безжалостно отвергнут, или попросту "уронит" канал, внеся сумбур и сумятицу в стройную цепочку бегущих друг за другом битов информации. Теоретически можно создать систему, перехватывающую тайм-слоты или даже целые контейнеры VC-12, но, во-первых, стоимость такой системы трудно себе представить, а во-вторых, все равно надо получить прямой физический доступ к сети, что само по себе нереально. Поэтому консервативные системы гораздо надежнее новых пакетных. Правда, народные умельцы все равно находили дыры в сложной технической системе аналоговой телефонии, чаще всего используя несовершенство системы обмена информации АОН. Чего только стоит знаменитый наделавший в свое время много шума прибор "Флай"... Но речь сейчас не об этом. В отличие от TDM-телефонии, сам принцип работы пакетной VoIP-телефонии априори предполагает многочисленные методы внедрения и взлома. IP-пакеты, получив последнее напутствие от софт-свича, как огромная толпа Красных Шапочек, по одиночке отправляются в дремучий лес, не зная, что их там ожидает и дойдут ли они вообще до любимой бабушки, т.е. до абонента. А по пути, как мы знаем из сказки Шарля Перро, может произойти все что угодно. Логично для начала построить им отдельную тропинку с заборчиком, отделив голос от всего остального. Поэтому наличие как минимум отдельных виртуальных локальных сетей VLAN, а лучше выделенных частных сетей VPN просто обязательно. VLAN или VPN создадут вам своего роде "трубу", в которую попадает только то, что

прописано в этой сети, и тем самым отделят ваш трафик от всего чужого. Крайне желательно также присвоить голосу свой приоритетный QoS (Quality of Service – уровень обслуживания), Это позволит промаркировать голосовые пакеты как приоритетные, как бы поставив им своеобразную депутатскую "мигалку". Это не прибавит вам безопасности, зато улучшит качество. Иначе при загруженной сети голосовые пакеты рискуют оказаться в банальной пробке, а для голосовых пакетов, как известно, очень важно не просто дойти до абонента, но дойти вовремя и выстроиться в правильную очередь, иначе звуки будут звучать не по порядку и вместо речи вы получите бессмысленную какофонию.

Идеальный случай расположения абонентских устройств внутри корпоративной сети реализуем далеко не всегда. Очень часто можно наблюдать случай, когда абоненту нужен именно ваш телефонный номер, например при переезде, а в новом месте нет вашей сети, зато есть Интернет другого оператора. Тогда до абонента можно "дотянуться" только через публичный Интернет. То есть абонентский шлюз стоит на "белом" адресе, открытый настежь, и защищен лишь паролем. Применение генератора паролей здесь строго обязательно. Пароль типа QWERTY – это открытая дверь в банковскую ячейку. Трафик между IP-АТС оператора и абонентом проходит много промежуточных цепей. Хакер, получивший доступ к одному из звеньев цепи, может подключить к нему монитор пакетов – сниффер и просмотреть все пакеты, пробегающие через это звено. Дальше – дело техники. Вычленить ваш пароль из огромной лавины информации сложно, но вполне возможно. Что делать? Первое, что приходит на ум, – это сделать так, чтобы публичный IP-адрес стал недоступным извне. Сделать это можно, поставив голосовой абонентский шлюз после маршрутизатора и закрыв его сервисом NAT (Nework Address Translation – замена сетевого адреса) и FireWall. Пробиться через NAT будет сложно, так как адрес ушел из публичной зоны и снаружи ничего уже не видно, FireWall же отражает слишком явные попытки взлома. Проблема вроде решена, но тут вылезает другая проблема: теперь оператор, не имея доступа внутрь сети, стоящей после маршрутизатора, теряет удаленное управление таким шлюзом и при возникновении проблемы не имеет возможности даже его перегрузить. Хорошо, если шлюз стоит на соседней улице, а если в другом городе? Тут, правда, есть возможность немного облегчить свое положение и "пробросить" через роутер порт управления внутрь на шлюз, но возможность настроить абонентский маршрутизатор выпадает далеко не всегда. Выбор между возможной потерей абонента, удобством обслуживания и опасностью взлома шлюза, как правило, в 100% случаев решается в пользу подключения. Прибыль от абонента при правильном подходе все равно покроет возможные издержки взлома. Поэтому первая заповедь при инсталляции и проектировании VoIP-сети – минимизировать стыки VoIP с публичными IP-сетями и применять его только в исключительных и неизбежных случаях и ни в коем случае не для основных узлов сети. Для этого лучше использовать внутреннюю сеть. Я знаю случаи построения корпоративных VoIP-сетей на полностью выделенной сети, где маршрутизаторы, коммутаторы DNS и прочие серверы используются только для голоса. Правда, все эти сети строились исключительно в рамках одного здания, и оператор вкладывал значительные финансы в построение такой сети, зато получал практически 100%-защищенную сеть. Чаще всего VoIP-сеть все же должна иметь выход в публичный Интернет. Мониторинг и тем более управление такой сетью необходимо осуществлять только через промежуточные узлы со сложной аутентификацией, которые служат буфером между внешней интернет-сетью и внутренней VoIP-сетью. Многие софт-свичи управляются через построенный на Java интерфейс, который, как правило, "крутится" на отдельном сервере. Для удобства управления доступ к такому серверу должен быть из любой точки, т.е. через тот самый небезопасный Интернет. Логично иметь одну такую Java-машину для управления, дать доступ к ней строго определенному кругу лиц и закрыть периодически меняющимися паролями.

Для тех элементов сети, которые все же оказались "снаружи", кроме упомянутого применения сложных паролей и возможного перемещения его на NAT можно посоветовать еще некоторые хитрости. Не так уж редки случаи, когда неопытные хакеры не знакомы с российским планом нумерации и, взломав шлюз, начинают делать наборы не с привычным нам префиксом 810, а с более привычными за рубежом двумя нулями. Правда, таких случаев в последнее время становится все меньше, взломщики стали опытнее и осведомленней. Поэтому рекомендацией здесь может быть применение только российского плана нумерации; даже в корпоративной сети нули для выхода в телефонную сеть общего пользования лучше не применять. Это хоть и небольшая,

скорее гипотетическая, но все же возможность защититься от несведущего хакера. Идеальным и беспроигрышным вариантом может послужить возможность биллинговой системы оператора по мониторингу превышения пикового лимита на некоторые направления, например, на острова Океании и Карибского бассейна, и отсылкой тревожного сигнала по SMTP или SMS. Далеко не каждая биллинговая система имеет такую возможность, но многие ее предоставляют, например относительно недорогой CombiBilling от T-Soft. Если ваш биллинг это позволяет, лучше воспользоваться такой возможностью. Некоторые софт-свичи имеют возможность мониторинга пиковой нагрузки на определенные префиксы и отсылки тревожного оповещения или блокировки наборов. Если ваш голосовой сервер имеет такую возможность, обязательно используйте ее. Также, если возможно, ограничьте число одновременных вызовов с одного аккаунта. Не бойтесь поздних звонков и SMS-сообщений, одна ночная SMS может спасти компанию от серьезных потерь. Иногда можно использовать встроенные в промышленные софт-свичи таблицы-расписания с разграничением возможности набора на некоторые направления и закрывать их на ночные часы. Также постарайтесь заранее выяснить у абонента, нужна ли ему международная связь, и если ответ будет отрицательным, то лучше вообще отключить ее в таблицах рестрикции.

Самой тяжелой потерей для оператора будет вскрытие базы данных, где хранятся данные аккаунтов абонентов. Для взломщика это настоящий клондайк, а оператору огромная головная боль – менять пароли на всех шлюзах. Аккаунты можно заводить где угодно и сколько угодно, даже не взламывая узлы, и лить туда трафик широкой рекой, подсчитывая свой доход. Такие базы данных надо хранить строже, чем Кащей Бессмертный хранил свою знаменитую иглу. Понятно, что записывать на блокнотике шариковой ручкой данные на тысячи абонентов – далеко не самый лучший вариант. Хранить его в чьей-то голове – тоже. Наверняка все помнят анекдот про админа, пытающегося с похмелья вспомнить пароль на роутер; здесь ситуация будет в тысячу раз хуже. Есть вариант применения одного и того же пароля для всех абонентов, но здесь важно, чтобы абоненты об этом, не дай Бог, не догадались, иначе серьезных разборок при выставлении счетов не избежать, так что вариант тоже далеко не самый лучший, тем более что при вскрытии менять пароли придется на всех шлюзах. Остается старый дедовский способ: хранить все данные в файле или БД под совершенно индифферентным именем в некоррелированной по смысловому имени директории на доступном только оператору сервере и доступ к этому файлу дать очень ограниченному числу лиц – это финансы компании.

Помимо взлома ради финансового обогащения, злоумышленники могут вскрывать VoIP и для других целей. Самым распространенным можно назвать прослушивание голосового тракта. Если злоумышленник по пути от софт-свича до абонента получает возможность "приложить ухо" к пропущенному трафику, в принципе возможно выделить нужные пакеты и декодировать голос. Метод и цель шантажа не входит в компетенцию данной статьи, главное, что у хакера появился компрометирующий или инсайдерский материал. Метод борьбы также прост. Не использовать устаревшие хабы, которые не коммутируют конкретные порты, а бездумно рассылают пакеты по всем портам, выключать ненужные порты на коммутаторах и обязательно использовать VLAN. Крайне осторожно надо применять так называемое зеркалирование портов коммутаторов, когда пакеты дублируются сразу в несколько портов по принципу хаба, ведь всегда есть вероятность включения в параллельный порт и снятия с него важной информации.

Совсем уж экзотикой выглядит инжектирование слов и звуков, искажающих первоначальный смысл сказанной фразы. Данный вид несанкционированного доступа настолько редок, что о нем трудно что-либо сказать. Сам по себе этот взлом априори предполагает много условий: схожесть тембра и уровня голоса, точное встраивание "инородных" пакетов в стройный ряд исходных пакетов, что само по себе сложная техническая задача. Метод борьбы схож с предыдущим случаем: не применять хабы, использовать VLAN, VPN, уводить в shutdown все неиспользуемые порты.

Самым грубым и брутальным можно считать, пожалуй, метод атаки на сервер или заражение его чем-то вредоносным. Про DDOS-атаки (Distributed Denial of Service) написано много и подробно, не думаю, что я могу сказать что-то новое. Суть атаки состоит в том, что сервер буквально заваливают ненужными запросами и он вынужден честно отвечать на все, не оставляя времени и ресурсов на основные задачи. Закрытие сервера файрволом, а еще лучше, вывод его из публичной сети, а также закрытие ненужных портов достаточно надежно защитят вас от DDOS. Схожая проблема

может возникнуть, если в сервер заслали "троянского коня". Самый свежий случай в моей практике, когда неожиданно упало качество связи. Внешне все хорошо, все работает, но голос в тракте идет с жуткими искажениями. Пока перебрали все параметры стыка на медиашлюзах, пока перепробовали все кодеки, перегрузили все, что может влиять на голос, ушло довольно много времени. Все это время раздраженные абоненты названивали и спрашивали, когда же, наконец, все починится. Причина была выявлена случайно и совсем не там, где искали. В сервер была загружена программа генерирования и расчета модной ныне виртуальной валюты – биткойнов, которая не отключила сервер и его сервисы, но здорово тормозила процессор и, как следствие, генерацию и передачу пакетов. Поэтому можно дать рекомендацию использовать отдельный сервер для ответственных VoIP-сервисов. Пусть лучше сервер будет попроще, но выделен специально для одного VoIP. Принцип прост: меньше сервисов – меньше открытых портов-сокетов, следовательно, меньше открытых дверей. Обязательно надо следить за обновлениями операционной системы, закрывающими дыры и уязвимости.

Помимо всего перечисленного нельзя также забывать о банальном регламенте допуска к VoIP-оборудованию. Здесь все как в жизни: чем больше бардака и элементарной халатности, тем выше риск получить неприятности. Каждый оператор должен сам выбрать золотую середину. Чем больше допущенного к оборудованию персонала, тем выше вероятность либо утечки информации (умышленной или неумышленной – не суть важно, главное – результат), либо элементарной нестыковки действий. С другой стороны, чем такого персонала меньше, тем выше риск в самый неподходящий момент попасть в ситуацию, когда вы просто не найдете квалифицированного специалиста для решения нештатной задачи. Следует опасаться открытых протоколов и использовать защищенные протоколы HTTPS или SSH. Можно порекомендовать вместо стандартного SIP-порта 5060 использовать любой другой, но защита эта скорее психологическая, чем реальная, вряд ли это всерьез остановит злоумышленников.

В целом, несмотря на все опасности, защита VoIP – дело не такое уж и сложное. Главное – учиться не на своих, а на чужих ошибках, оценивать риски и идти вперед. ■