Методы обнаружения вторжений в киберсистемы цифровой обработки сигналов

С. А. Петренко

Успехи микропроцессорной технологии привели в 1990-х гг. к массовому переходу учрежденческих АТС (УАТС) среднего и крупного размера на цифровую обработку вызовов. Более того, непосредственно в настоящий момент наблюдается еще один качественный переход в области корпоративной телефонии — от «традиционных» цифровых АТС к IP-телефонии. При этом пропорции всех трех технологий (аналоговая, цифровая, IP-телефония) в парке работающих УАТС практически сравнялись. При неоспоримо большем спектре возможностей, предоставляемых абоненту цифровой телефонной линией, необходимо учитывать и целый спектр вопросов, связанных с защитой речевой информации, порождаемый цифровой обработкой вызовов и голоса.

Цифровая схема передачи сообщений (как управляющих, так и голосовых) на практике не только не устраняет характерные для традиционных схем угрозы, но и порождает целые классы новых угроз нарушения конфиденциальности. Пожалуй, единственным преимуществом цифровой (в т. ч. IP-) обработки голоса в этом аспекте является потенциальная готовность схемы к прозрачному внедрению программных средств криптографической защиты речевой информации. Однако этот процесс в отношении УАТС общего (неспециального) назначения только начинает свое развитие. В данной статье проведен анализ наиболее вероятных к реализации угроз нарушения конфиденциальности речевой информации в цифровых и IP-УАТС.

1. Угроза подключения в пределах коммутационной матрицы

Цифровая обработка сигналов дает возможность копирования («ответвления») голосового трафика в пределах коммутационной матрицы без каких бы то ни было демаскирующих признаков. Факт копирова-

ния невозможно отследить, он не вызывает ни изменений в амплитуде передаваемого сигнала, ни искажений, связанных с задержкой передачи. Это является качественным отличием цифровых систем телефонии от систем предыдущего поколения.

Практически все крупные разработчики оборудования для УАТС реализовали в программном обеспечении те или иные возможности копирования речевого трафика при наличии у прослушивающей стороны соответствующих полномочий, определенных администратором телефонной станции. В некоторых случаях это полноценная трехсторонняя конференц-связь с отключенным входящим голосовым каналом от прослушивающей стороны, в других — ответвление потока по специальной схеме при наборе определенного номера. Некоторые исследователи в области информационной безопасности отдельно выделяют так называемый «полицейский режим» — возможность выполнения тех же операций извне, при наборе из городской телефонной сети определенного номера, принадлежащего номерному полю УАТС, и кода допуска. Рассмотрим реализацию данных технологий в некоторых широко распространенных моделях телефонных станций.

Цифровые учрежденческие АТС модели AVAYA Definity реализуют возможность скрытого копирования речевой информации в рамках возможности «Service Observing» (Контроль вызова), позиционируемой как средство для контроля со стороны менеджеров за ходом работы телефонных операторов, в первую очередь в Центрах обработки вызовов. Активация функции возможна как в варианте с подачей в речевой канал предупредительного сигнала каждые 12 секунд о факте прослушивания третьей стороной, так и без него. Настройка полномочий на прослушивание выполняется с консоли администратора по групповому принципу : каждой абонентской линии соотносится класс приоритетов «COR», а в матричной форме для каждой пары классов определяется разрешение или запрет прослушивания. Активация прослушивания выполняется набором кода доступа к сервису, а затем номера абонента, и может быть назначена на одну из функциональных клавиш прослушивающего аппарата. Кроме того, при определенной настройке возможен доступ к функции с внешних линий, например, с городской телефонной сети.

Сервер IP-телефонии CallManager от компании Cisco Systems Inc. также предоставляет возможность включения в разговор третьего абонента, обладающего достаточными полномочиями (как с предупредительным сигналом, так и без него). Функция именуется «Barge In» и имеет две различные схемы технической реализации.

1. Схема на основе программно-аппаратных средств, штатно встроенных во все IP-аппараты компании с 2-мя линиями. Прослушиваемый IP-аппарат при поступлении запроса на конференц-связь (в т. ч. одностороннюю — прослушивание) самостоятельно выполняет ответвление и микширование двух голосовых потоков (первичного — в направлении абонента и вторичного — в направлении прослушивающего устройства) аппаратными средствами второй линии. При этом при соответствующей настройке предупредительных сигналов в первичный голосовой поток не добавляется, более того, на дисплее прослушиваемого IP-аппарата не появляется никаких информационных признаков о факте подключения. Данная схема ограничена только одним подключением прослушивания и только широкополосным (64 кбит/с) кодеком G.711, однако не вносит никаких демаскирующих искажений в голосовой поток.
2. Схема на основе выделенных программно-аппаратных средств конференц-связи сервера IP-телефонии. При поступлении запроса сервер IP-телефонии замыкает голосовой трафик в обоих направлениях (проходивший до этого момента напрямую между IP-устройствами) на устройство конференц-связи и с его помощью выполняет микширование и ответвление данных (в этом случае уже на неограниченное количество прослушивающих устройств и вне зависимости от используемого абонентами кодека). Недостатком схемы по сравнению с первым вариантом является слышимое искажение («провал голоса») в момент переключения потоков.

Настройка привилегий на прослушивание выполняется отдельно для каждой прослушиваемой линии (непосредственно указывается набор линий, имеющих право на подключение, в т. ч. незаметное, к разговору).

Таким образом, получение злоумышленником тем или иным образом привилегий администратора цифровой УАТС (например, посредством успешной атаки на его персональный компьютер) предоставляет ему практически неограниченные возможности по незаметному прослушиванию ведущих телефонных переговоров.

2. Угроза прослушивания разговоров в помещении с помощью автоответа

Цифровые и IP-аппараты, как сложные компьютерные устройства, привнесли еще один класс угроз утечки речевой информации, связанный с возможностью удаленного (в т. ч. при некоторых условиях —

несанкционированного) включения микрофона и передачи разговоров, ведущихся в помещении по цифровому каналу. В качестве первого рассмотрим вариант, не связанный с недокументированными возможностями самих аппаратов — широко распространенную опцию «Автоответ». При ее активации вызываемый аппарат при поступлении вызова подает один (часто — укороченный) сигнал вызова, а затем автоматически включает микрофон и громкоговоритель с тем, чтобы абоненты имели возможность общаться между собой по громкой связи либо с использованием гарнитуры.

При возможности настройки опции «Автоответ» в зависимости от вызывающей линии (интерком) она начинает представлять реальную угрозу прослушивания разговоров, ведущихся в помещении. Злоумышленник, получивший привилегии администрирования УАТС, может создать интерком-группу, включив в нее атакуемую линию и свой номер, изменить сигнал вызова со своей линии на запись тишины и получить тем самым возможность прослушивать разговоры в помещении, сделав вызов на данную линию. Схема обладает некоторыми незначительными демаскирующими признаками : 1) в зависимости от модели аппарата факт включения микрофона может отражаться индикаторами, 2) линия в момент прослушивания будет занята при попытке вызова извне, и 3) существует риск поднятия прослушиваемым абонентом трубки для выполнения вызова. Однако это не исключает возможность выполнения успешного и скрытного прослушивания, особенно в ситуациях, когда в помещении идет активное обсуждение того или иного вопроса, а телефонный аппарат установлен так, что его индикаторы не видны присутствующим.

3. Угроза наличия недокументированных возможностей управления аппаратом

Недокументированные возможности самих аппаратов (в особенности IP-) являются еще одной угрозой для конфиденциальности речевой информации в защищаемых помещениях. Программное обеспечение IP-телефонов представляет собой сложный программный комплекс, в т. ч. реализующий стек протоколов TCP/IP, и может содержать:

- недокументированные возможности, внесенные разработчиками в целях тестирования или на определенных этапах разработки новых функциональных возможностей аппаратов;

- ошибки в реализации, например, приводящие к уязвимостям класса «переполнение буфера» и позволяющие получить полный контроль над программным обеспечением аппарата до его перезагрузки.

Примером угрозы первой группы является имевшаяся в одной из версии ПО возможность отправки на IP-телефоны наиболее популярных моделей 7940 и 7960 компании Cisco Systems Inc. управляющего XML-сообщения CiscoIPPhoneExecute, которое среди прочих возможностей (набор номера, эмуляция нажатия клавиш и т. п.) могло включать микрофон аппарата и передавать весь голосовой трафик на указанный в XML-сообщении IP-адрес.

4. Угроза прослушивания IP-трафика в момент передачи по сети

Различные варианты реализаций угроз прослушивания трафика традиционны для компьютерных сетей, использующих в своей структуре широковещательные сегменты (Ethernet, в т. ч. коммутируемый, радио-Ethernet и т. п.), и создают еще один уровень возможных атак на системы IP-телефонии. При отсутствии шифрования трафика на сетевом или более высоких уровнях модели OSI существует несколько вариантов нарушения конфиденциальности передаваемых сообщений.

В условиях отсутствия у злоумышленника административных прав на активное сетевое оборудование наиболее эффективной в коммутируемых Ethernet-сетях является атака «ARP spoofing», выполняющая изменение таблицы маршрутизации на канальном (MAC) уровне с помощью специально сформированных ARP-пакетов. Также к раскрытию определенной части передаваемой информации может привести перевод коммутатора в режим концентратора с помощью большого количества фальшивых пакетов (MAC-storm), хотя этот способ и обладает значительными демаскирующими признаками, выражающимися в резком снижении качества работы сети.

При получении злоумышленником административных прав на коммутирующем или маршрутизирующем оборудовании (например, в результате атаки на компьютер администратора или при перехвате его пароля, передавшегося в открытом виде) у него появляются гораздо более мощные средства перехвата IP-трафика. Они включают :

- возможность активации на коммутаторах зеркальных (SPAN) портов, получающих точную копию передаваемого по определенным портам трафика;
- использование иных технологий «ответвления» трафика от производителей сетевого оборудования, например:
  – протокола ERSPAN (Encapsulated Remote SPAN), инкапсулирующего каждый перехватываемый пакет в пакет протокола GRE, что позволяет передавать его по IP-сетям без каких-либо ограничений дальности;
  – опции IP Traffic Export, реализующей «ответвление» трафика при его маршрутизации на 3-м уровне модели OSI;

  (оба протокола поддерживают возможность тонкой настройки фильтрации перехватываемых пакетов, что позволяет копировать трафик только от определенных групп IP-устройств).

Беспроводные сети при отсутствии стойких алгоритмов шифрования также являются потенциальным источником раскрытия передаваемого по ним голосового трафика.

5. Угроза подмены сообщений в управляющем канале IP-телефонии

Методика централизованного управления IP-телефонными вызовами (реализуемая в УАТС) содержит еще один возможный путь прозрачного для абонентов перехвата их разговоров. В момент установления IP-соединения первоначальный обмен информацией, содержащей номера абонентов, их имена, технические возможности аппаратов и т. п., в т. ч. IP-адреса оконечных устройств, идет между серверами IP-телефонии (см. рис. 1). На этом этапе возможна подмена (средствами атак сетевого уровня) информации об одном или обоих IP-адресах с целью внедрения компьютера злоумышленника в цепочку передачи голосового трафика по принципу прозрачного прокси-сервера.

Подобный класс атак остается совершенно незаметным на прикладном уровне, т. к. пользователю обычно не видны сетевые координаты удаленного абонента, а стек протоколов не способен обнаружить факт подмены, и может быть выявлен только с помощью специализированного мониторинга сетевого трафика.

В целом, предпосылкой для появления возможности подобных атак является то, что в современных протоколах IP-телефонии (H.323,

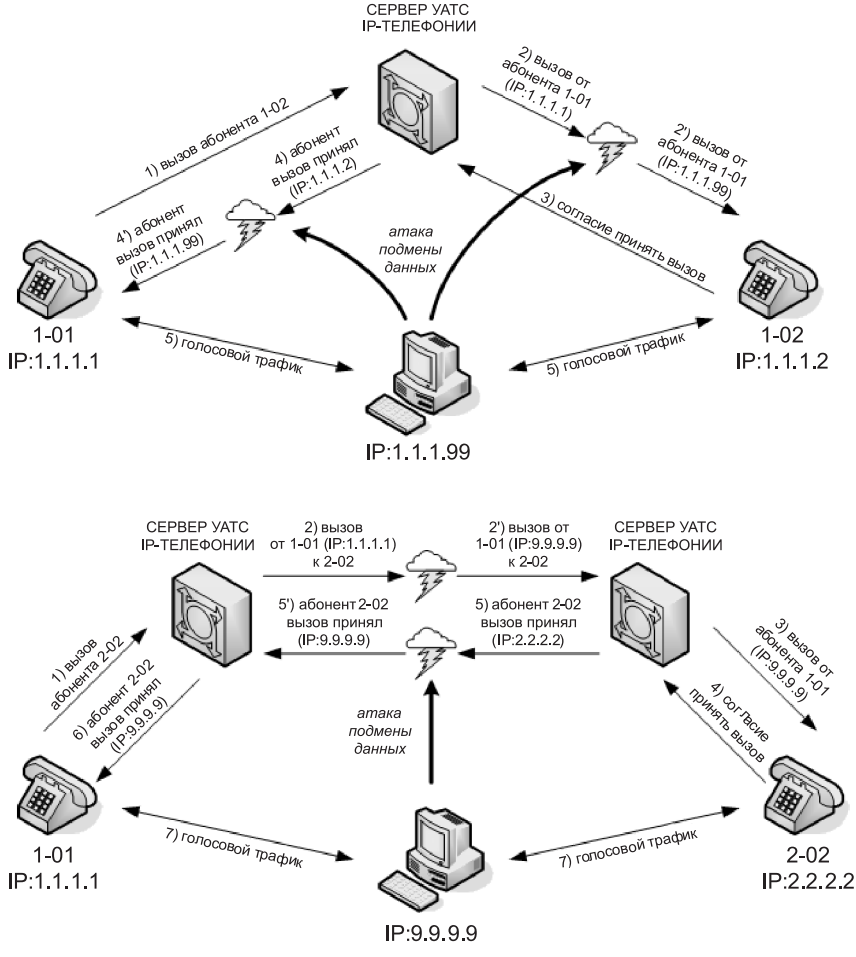

Рис. 1. Установление IP-соединения

SCCP и др.) оконечное оборудование при приеме и передаче голосового потока является ведомым относительно сервера УАТС, и полностью полагается на информацию, сообщенную ему в управляющем канале (в т. ч., например, не проверяет соответствие IP-адресов отправителя и получателя голосового потока в рамках одного и того же разговора). Проблема обеспечения защиты от внедрения в голосовой поток прокси-сервера поднимает вопрос об обеспечении целостности передаваемых в управляющем канале данных стойкими криптографическими методами.

6. Выводы

Смена технологий в области телефонии для объектов информатизации от аналоговым к цифровым, а затем и к IP-устройствам породила ряд новых угроз конфиденциальности речевой информации как передаваемой средствами УАТС, так и циркулирующей в помещениях с установленным оконечным телефонным оборудованием. Данная проблема требует разработки и внедрения новых методов, средств и методик контроля за режимом функционирования УАТС и их распределенных компонентов, а также приемов мониторинга несанкционированных воздействий и аномалий в компьютерных сетях, передающих трафик IP-телефонии. Ряд названных методик был разработан и опробован автором на практике. Анализ полученных результатов свидетельствует об актуальности указанного направления защиты речевой информации в цифровых и IP-учрежденческих АТС.

Литература

1. *Петренко С. А., Курбатов В. А.* Политики информационной безопасности. М.: ДМК Пресс, 2006. 400 с.: ил. (Информационные технологии для инженеров).
2. *Петренко С. А., Симонов С. В.* Управление информационными рисками. Экономически оправданная безопасность. М.: ДМК Пресс, 2005. 384 с.: ил. (Информационные технологии для инженеров).
3. *Петренко С. А., Петренко А. А.* Аудит безопасности Intranet. М.: ДМК Пресс, 2002. 416 с.: ил. (Информационные технологии для инженеров).
4. *Мамаев М. А., Петренко С. А.* Технологии защиты информации в Интернете. Специальный справочник. СПб: Питер, 2002. 848 с.: ил. (Специальный справочник).