УДК 004.056

А.А. Нечай[1]
П.Е. Котиков[2]

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННЫХ АВТОМАТИЧЕСКИХ ТЕЛЕФОННЫХ СТАНЦИЯХ

Статья посвящена актуальному вопросу, обозначенному в заголовке. Представлен анализ влияния применения достижений цифровой техники в АТС на защищенность информации. Наиболее подробно освещены варианты сценариев информационных атак. Ценным является также рассмотрение конкретных технологий информационного воздействия.

Ключевые слова: *АТС (автоматическая телефонная станция), информация, цифровая обработка, защищенность информации, цифровая схема.*

A.A. Nechai
P.E. Kotikov

ACTUAL PROBLEMS OF INFORMATION PROTECTION IN MODERN AUTOMATIC TELEPHONE STATIONS

The article is devoted to the topical issue, marked in the headline. The analysis of effect of applications of digital technology in automatic telephone-exchange on secure information is presented. The scenarios of information attaks are highlighted in details. Valuable is also the consideration of specific technologies of informational influence.

Keywords: *ATE (automatic telephone-exchange), information, digital processing, information security, digital circuit.*

Успехи микропроцессорных технологий привели к массовому переходу автоматических телефонных станций (АТС) на цифровую обработку вызовов. Более того, непосредственно в настоящий момент наблюдается еще один качественный переход в области ведомственной телефонии – от «традиционных» цифровых АТС к IP-телефонии. При этом пропорции всех трех технологий (аналоговая, цифровая, IP-телефония) практически сравнялись.

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 том числе 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.

Существует множество механизмов осуществления атак на АТС. При этом задачи, преследуемые нарушителями, могут сильно отличаться, а именно:

– получение коммерческого эффекта от воровства услуг телефонных переговоров;

– осуществление скрытого съема информации, содержащей коммерческую или государственную тайну;

– выведение оборудования телефонной сети из строя.

Наибольшую опасность может представлять несанкционированный доступ злоумышленников к программным портам АТС через внешние каналы телефонной связи. Для осуществления указанных действий в программное обеспечение телефонных станций встраиваются скрытые мо-

[1] Преподаватель Военно-космической академии им. А.Ф. Можайского.

[2] Кандидат технических наук, доцент Военно-космической академии им. А.Ф. Можайского.

дули («закладки»). Командами запуска «закладок» могут являться специальные сообщения, скрытно передаваемые по служебным или пользовательским каналам. В результате реализации указанных действий злоумышленник получает полный контроль над АТС, включая возможность дистанционного съема информации и полного вывода оборудования из строя. В мировой и отечественной практике существует множество реальных фактов обнаружения «закладок» в коммутационном оборудовании зарубежного производства (информация о некоторых из них приведена в СМИ).

Закладки, реализующие упомянутые функции, весьма сложно выявить. Гарантию того, что в коммутационных станциях отсутствуют недекларированные возможности, может дать экспертиза их принципиальных схем и исходных текстов ПО, которая проводится только при сертификации изделий.

Выделим и опишем следующие типовые угрозы цифровых и IP- АТС информатизации:

1. Подключение 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 копирования 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 конференцсвязь 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 каждые 12 секунд предупредительного сигнала 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 двумя линиями. Прослушиваемый IP-аппарат при поступлении запроса на конференцсвязь (в том числе 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 конференцсвязи 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. Прослушивание 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 том числе 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.

3. Наличие недокументированных возможностей

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 том числе 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 версиЙ ПО возможность отправки на IP-телефоны наиболее популярных моделей 7940 и 7960 компании Cisco Systems Inc. управляющего XML-сообщения CiscoIPPhone-Execute, 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. Прослушивание IP-трафика при передаче по сети

Различные варианты реализаций угроз прослушивания трафика традиционны для компьютерных сетей, использующих в своей структуре широковещательные сегменты (Ethernet, в том числе 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, передававшегося 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-ем 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. Подмена 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 том числе IP-адреса оконечных устройств, идет между серверами IP-телефонии. 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, так как 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, 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 (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.

Выводы

1. Смена технологий в области телефонии для объектов информатизации от аналоговых 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. Это требует разработки и внедрения новых методов, средств и методик контроля над режимом функционирования УАТС и их распределенных компонентов, а также приемов мониторинга несанкционированных воздействий и аномалий в компьютерных сетях, передающих трафик IP-телефонии. Анализ полученных результатов подтверждает актуальность разработки программно-аппаратного комплекса автоматического контроля настроек УАТС и ТА (абонентских линий) КВО информатизации.

2. Необходимо отметить, что абсолютно надежных систем защиты не существует. Кроме того, любая система защиты увеличивает время доступа к информации, поэтому построение защищенных КС не ставит целью надежно защититься от всех классов угроз.

3. Уровень системы защиты – это компромисс между понесенными убытками от потери конфиденциальности информации, с одной стороны, и убытками от усложнения, удорожания КС и увеличения времени доступа к ресурсам от введения систем защиты, с другой стороны.

Литература

1. Петренко А.С., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. – М. : ДМК Пресс, 2005. – С. 384.

2. Мамаев М.А., Петренко С.А. Технологии защиты информации в Интернете. Специальный справочник. – СПб. : Питер, 2002. – С. 848.

3. Лохвицкий В.А. Подход к построению системы автоматизированной интеграции информации в базу данных для её своевременной актуализации / В.А. Лохвицкий, С.В. Калиниченко, А.А. Нечай // Мир современной науки. – 2014. – № 2 (24). – С. 8–12.

4. Нечай А.А. Выявление недекларированных возможностей аппаратно-программного обеспечения / А.А. Нечай // Экономика и социум. – Саратов, 2014. – № 1–2 (10). – С. 457–460.

5. Нечай А.А. Специфика проявления уязвимостей в автоматизированных системах управления критически важными объектами / А.А. Нечай, П.Е. Котиков // Современные тенденции в образовании и науке : сборник научных трудов по материалам Международной научно-практической конференции : в 14 частях. – Тамбов, 2014. – С. 96–97.

6. Скородумов Б.И. Современные проблемы отечественного профессионального стандарта информационной безопасности / Б.И. Скородумов // Вестник Российского нового университета. – 2014. – № 4. – С. 156–158.