УДК 621.391

АНАЛИЗ УЯЗВИМОСТЕЙ СЕТИ VoIP НА БАЗЕ NGN К УГРОЗАМ НЕЛЕГИТИМНЫХ СИГНАЛЬНЫХ И МЕДИАСООБЩЕНИЙ

А.М. Морозов, ведущий инженер отдела управления сетями Регионального центра управления сетями связи Московского филиала ОАО «Ростелеком»; a.m.morozov@gmail.com

Ключевые слова: *сети связи нового поколения (NGN), угроза, отказ в обслуживании, передача голоса по IP-сетям, протокол инициирования сеанса (SIP), программный коммутатор, компрометация, медиашлюз.*

Введение. Настоящая работа посвящена анализу уязвимостей сети передачи голоса по IP-сетям (Voice over IP, VoIP) [1], построенной на основе архитектуры сети связи следующего поколения (New Generation Network, NGN), широко применяемой операторами связи. Ряд особенностей NGN создают предпосылки для реализации угроз безопасности. Это, во-первых, использование нескольких типов протоколов, таких как протоколы управления соединением (Session Initiation Protocol (SIP), а также протоколы группы SIGTRAN), протоколы управления медиашлюзами (MGCP, MEGACO/H.248), передачи медиаданных и управления медиапотоками (RTP/RTCP). Другой особенностью NGN является распределенная архитектура сети, когда ее отдельные компоненты могут находиться в разных IP-сетях и разных административных доменах сети.

Испытания уязвимости к некоторым угрозам информационной безопасности (ИБ) проводились на сети одного из российских операторов сети связи общего пользования, работающей по протоколу сигнализации SIP. Имитировались следующие угрозы ИБ:

- нелегитимные сигнальные сообщения – запросы и ответы (компрометация сигнальных сообщений). В сети сигнализации SIP такими сообщениями, например, могут быть запросы CANCEL, BYE, а также сообщения-ответы об ошибках в ходе установления соединения;
- нелегитимная полезная нагрузка сигнальных сообщений (компрометация полезной нагрузки сигнальных сообщений), в частности передача в сигнальных сообщениях некорректных данных для установления медиасессии. В результате реализации такой угрозы возникает ситуация, при которой соединение устанавливается, но обмен данными в рамках этой сессии невозможен или возможен с существенными ограничениями;
- нелегитимные медиасообщения. При большом потоке указанных сообщений имитировалась атака «отказ в обслуживании» (Denial of Service, DoS).

Компрометация сигнальных сообщений. Данный вид угрозы ИБ сводится к тому, что в сторону компонента сети SIP отправляется скомпрометированный запрос или скомпрометированный ответ на запрос, в результате обработки которого компонент сети NGN, подвергшийся атаке, разрывает соединение.

На рис. 1 приведена схема проведения испытаний на тестовом участке сети SIP, в ходе которых имитировалась угроза, реализованная путем компрометации запроса CANCEL.

Алгоритм реализации атаки следующий:

F1 – SIP-абонент (легитимный абонент программного коммутатора SSW test) инициирует сессию;

F2 – программный коммутатор (SSW test) подтверждает получение запроса на установление сессии и начало его обработки;

F3 – злоумышленник (SIP-терминал, имитирующий злоумышленника) от имени легитимного пользователя-инициатора сессии направляет на сервер запрос CANCEL, который дает программному коммутатору команду на прекращение обработки запроса INVITE;

F4–F6 – сессия завершается.

Реализация данного вида атаки для злоумышленника осложняется необходимостью обеспечить в компрометируемых сообщениях соответствие идентификационных данных диалога идентификационным данным того диалога, на прекращение которого эти сообщения нацелены. Поэтому такой вид угрозы в действующих сетях чаще всего возникает как непреднамеренный. Но в этом случае уместно говорить не о компрометации, а об ошибочной передаче запросов на прекращение соединения. Причиной могут быть ошибки программного обеспечения или конфигурации компонентов сети SIP. Также данный вид атаки может быть использован злоумышленником как этап реализации других угроз безопасности, например угрозы мошенничества.

Компрометация полезной нагрузки сигнальных сообщений. Преднамеренное или непреднамеренное изменение данных, содержащихся в теле сигнальных сообщений, может привести к отказу в установлении соединения или к ошибкам при установлении соединения, в результате которых передача полезной информации становится невозможной.

Рассмотрим примеры реальных ситуаций, возникающих на действующей сети в результате неправильной конфигурации программного коммутатора и медиашлюза или сбоя в программном обеспечении.

На рис. 2 приведен пример сигнального обмена, когда из-за программной ошибки один из участников сессии не мог выполнить выбор медиакодека, что приводило к срыву соединения.

Сценарий сигнального обмена:

F1 – программный коммутатор (softswitch) ssw1 направляет программному коммутатору ssw2 действующего сегмента сети запрос INVITE на установление сессии. В теле данного запроса содержатся конфигурационные данные (в формате протокола sdp), необходимые для приема медиапотока на стороне ssw1, в том числе набор медиакодеков, доступных программному коммутатору ssw1 (на рисунке изображен только набор возможных медиакодеков).

F2 – программный коммутатор ssw2 подтверждает получение запроса на установление сессии и начало его обработки.

F3 – программный коммутатор ssw2 направляет предварительный информационный ответ, содержащий конфигурационные данные ssw2 для приема медиапотока. Протоколом SIP [2] предписывается, что в этом ответе ssw2 должен сообщить о единственном кодеке, выбранном из списка кодеков, содержащихся в запросе INVITE для организации медиапотока. Однако ssw2 в этом ответе направляет на ssw1 свой список доступных кодеков.

F4 – программный коммутатор ssw1, получив в ответе 183 Call progress список доступных программному коммутатору ssw2 медиакодеков, выбирает единственный кодек, доступ-

Рис. 1. **Компрометация запроса CANCEL**

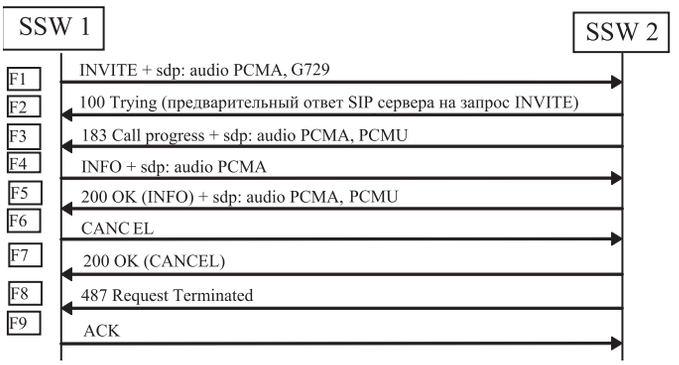

Рис. 2. **Срыв сессии при возникновении ошибки с выбором кодека**

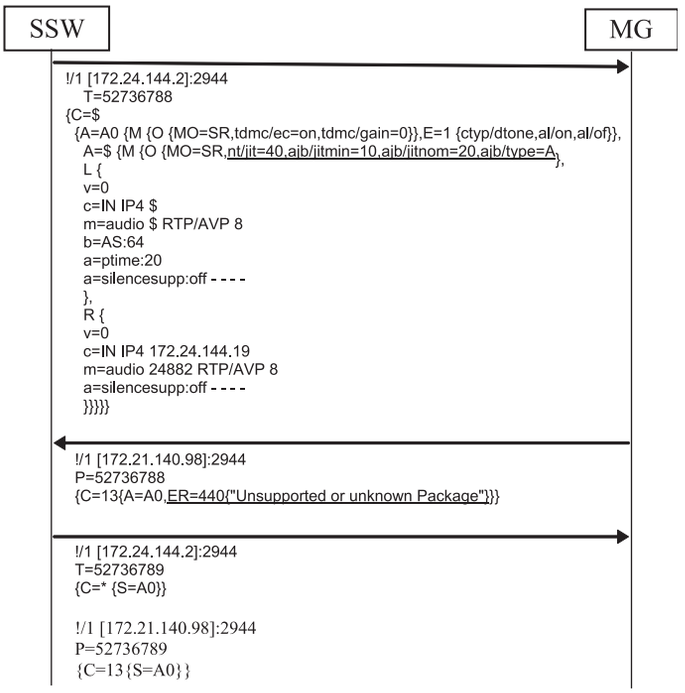

Рис. 3. **Отказ в установлении соединения из-за несовпадения программных реализаций протокола MEGACO и конфигурационных данных**

ный обоим программным коммутаторам, и сообщает о своем выборе запросом INFO.

F5 – программный коммутатор ssw2 подтверждает получение запроса INFO, но в теле ответа повторно передает список доступных медиакодеков, сообщая тем самым, что необходимый для организации медиапотока кодек не выбран.

F6 – в связи с тем, что в ходе установления сессии однозначно определить медиакодек для передачи медиапотока не удалось, программный коммутатор ssw1 посылает запрос на прекращение установления сессии (CANCEL).

F7–F9 – сессия завершается.

На рис. 3 приведен пример сигнального обмена по протоколу MEGACO [3], при котором от программного коммутатора на медиашлюз поступает команда на создание соединения, но наличие в команде неизвестного медиашлюзу параметра приводит к сбою в установлении соединения.

В концепции протокола MEGACO каждое соединение представляет собой так называемый контекст – логическую сущность, объединяющую необходимое для организации соединения количество терминальных окончаний (физических и логических портов с набором характеристик, атрибутов и режимов их работы), обеспечивающих организацию медиапотока.

При выполнении нового соединения программный коммутатор (на схеме обозначен SSW) передает медиашлюзу MG (Media Gateway) команду на создание нового контекста и добавление в него необходимого количества терминальных окончаний, устанавливает их режимы, дополнительные атрибуты и параметры для организации медиапотока. Медиашлюз выполняет поступившие команды, подтверждает их выполнение или информирует программный коммутатор о невозможности сделать это.

На рис. 3 программный коммутатор отправляет медиашлюзу команду на создание контекста. В ряду параметров, необходимых для организации медиапотока, программный коммутатор передает параметры буфера задержки (djitter buffer) – на схеме эти параметры в запросе программного коммутатора выделены подчеркиванием. Однако данные параметры вызывают сбой в обработке сообщения медиашлюзом и медиашлюз возвращает сообщение об ошибке. В ответе медиашлюза сообщение о причине сбоя также выделено подчеркиванием. После получения от медиашлюза сообщения об ошибке программный коммутатор прекращает процедуру установления соединения и дает команду на удаление контекста. Медиашлюз подтверждает выполнение команды на удаление контекста.

Рассмотренная ситуация стала следствием несовпадения программной реализации протокола MEGACO на программном коммутаторе и медиашлюзе и связанных с этим несоответствием различий конфигурационных данных.

Анализ испытаний уязвимостей к атакам DoS сети VoIP по каналам медиасообщений. В сети VoIP трассы прохождения сигнальных сообщений и медиаданных различаются. В то время как сигнальные сообщения замыкаются на программном коммутаторе, который реализует функции обработки сигнализации и управления соединениями, медиаданные передаются между участниками соединения медиашлюзами напрямую (рис. 4).

Медиашлюз реализует функции кодирования и транскодирования медиаданных, их трансляции между IP-сетью и абонентом, а также между IP-сетью и сетью ТфОП. Для организации медиапотока в рамках каждой сессии на медиашлюзе динамически определяются параметры медиасессии, такие как тип медиаданных, используемый кодек, период пакетизации, режимы эхо-компенсации и пр. В том числе выделяется транспортный адрес, состоящий из пары «IP-адрес и UDP/TCP-порт». Эти значения медиашлюз с помощью сообщений сигнализации передает предполагаемому участнику устанавливаемой сессии.

Существует угроза DoS-атаки на медиашлюз по каналам медиаданных, которая обусловлена следующими факторами:

1. Сигнальные сообщения протоколов управления соединениями и протоколов управления медиашлюзами передаются по сети в открытом виде и могут быть перехвачены злоумышленником, в результате чего ему станет известен транспортный адрес медиашлюза (IP-адрес и UDP/TCP-порт), на который медиашлюз готов принимать медиаданные.

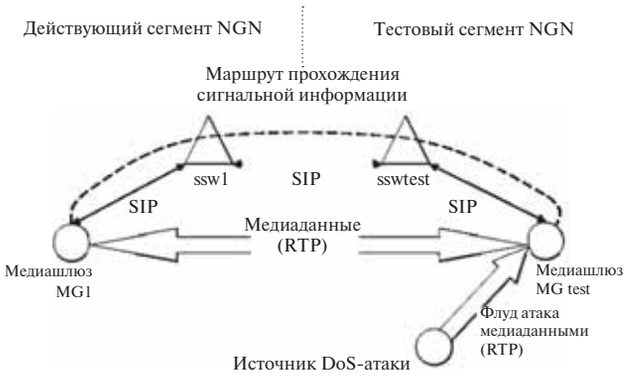

Рис. 4. **Имитация флуд-атаки медиаданными**

2. Распределенная архитектура NGN-сети предполагает, что ее различные компоненты могут находиться в разных IP-сетях и разных административных доменах сети. Необходимость обеспечить IP-доступность всех компонентов NGN-сети осложняет реализацию политик безопасности и формирует предпосылки для возникновения различных угроз безопасности, в том числе флуд-атаки посредством передачи интенсивного потока медиасообщений на медиашлюз оператора связи.

На рис. 4 представлена схема имитации флуд-атаки медиаданными. Перехватив информацию о транспортном адресе медиашлюза MG test, злоумышленник (на схеме обозначен как «Источник DoS-атаки») организует передачу на этот адрес медиапотока. Поток медиаданных от злоумышленника препятствует корректной обработке медиаданных, поступивших от легитимного пользователя (медиашлюза MG1), что приводит к значительному ухудшению качества.

При реализации данного типа атаки в сигнальном обмене аномалий не наблюдается. Для злоумышленника осуществление такой атаки не сопряжено с необходимостью обеспечивать соответствие передаваемых им данных каким-либо идентификационным параметрам легитимного медиапотока. Это значительно снижает техническую сложность реализации такой атаки, а ее выявление и локализация требуют скрупулезного анализа потока медиаданных.

Заключение. Проведенные испытания позволяют оценить степень уязвимости сети передачи голоса по IP (VoIP) к различным типам угроз, а также выявить признаки начала и развития исследуемых DoS-атак. Результаты данного исследования могут быть использованы при разработке алгоритмов раннего обнаружения угроз информационной безопасности. Целесообразно продолжить тестирование сетей передачи голоса по IP (VoIP) операторов связи с применением имитации различных типов атак для поиска методов раннего обнаружения угроз информационной безопасности и механизмов надежного противодействия этим угрозам.

ЛИТЕРАТУРА

1. **Дэвидсон Д. и др.** Основы передачи голосовых данных по сетям IP. – М.: Вильямс, 2007.
2. **Schulzrinne H. and others.** SIP: Session Initiation Protocol //RFC 3261. – June 2002.
3. **Cuervo F. and others.** MEGACO Protocol Version 1.0 //RFC 3015. – November 2000.

Получено 18.03.13