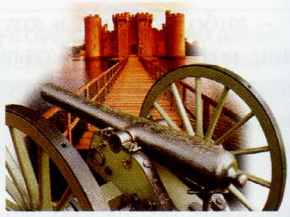
Безопасность и фрод-контроль в сетях NGN/IMS



Окончание. Начало см. «ИКС» № 1–2, с. 64.

Илья ЕХРИЕЛЬ, технический директор «НТЦ СевенТест», канд. техн. наук
Эдуард БАЖЕНОВ, начальник отдела разработки решений OSS/BSS, «НТЦ СевенТест»
Владислав КОЛЕСНИК, заместитель начальника отдела разработки решений OSS/BSS, «НТЦ СевенТест»

Применение протоколов IP и SIP, а также разнообразие механизмов доступа делает сети NGN/IMS уязвимыми для DoS-атак и фрода. Для противодействия этим угрозам безопасности необходимы комплексные системы с функциями кросс-анализа всех используемых протоколов и подсистем.

Примеры реализации DoS-атак в IMS

Защита от DoS/DDoS-атак – одно из требований к системе безопасности, отсутствующих в стандартах IMS. Хотя в IMS существует механизм аутентификации абонентов с помощью IPsec и SIP Digest, а также авторизация доступа абонентов к услугам через HSS, но и легитимные абоненты имеют возможность генерировать атаки на инфраструктуру IMS. Причем эти атаки могут опираться на сообщения протокола SIP, на сообщения протокола RTP или обоих сразу.

В сравнении с интернет-атаками анонимных абонентов вероятность атак на инфраструктуру IMS несколько меньше, поскольку абоненты имеют договорные отношения с поставщиком услуг и системе известны. Однако с точки зрения потери доходов оператора, оттока абонентов и даже угрозы человеческой жизни (если затронуты услуги экстренных служб) последствия успешных атак могут быть даже более тяжелыми.

Одна из услуг IMS – определение статуса присутствия (многими сейчас рассматривается как база для создания массы коммерчески интересных услуг) – позволяет информировать подписчика о том, находятся ли другие пользователи в онлайне, а также о доступных в данный момент возможностях для связи с ними. Когда пользователь заказывает такую услугу относительно интересующих его абонентов, производится обмен транзакциями SUBSCRIBE и NOTIFY с серверами услуги присутствия, которые управляют информацией о статусе каждого из абонентов.

Для уменьшения количества транзакций в процессе заказа используется специальная функция, но вместо нее злоумышленник может взять длинный список легального абонента и вызвать посылку сотен сообщений к серверу услуги присутствия. Задействуя одновременно длинные списки большой группы абонентов, можно организовать на сервер присутствия DDoS-атаку.

В IMS маршрутизация и тарификация многих услуг (присутствия, VoIP, push-to-talk) осуществляется через CSCF. В результате нарушение работы сервера присутствия по причине DDoS-атаки может вызвать задержку обработки трафика других услуг. Ведь если ответ от сервера присутствия не получен в течение определенного спецификацией протокола SIP таймера (32 с), то каждый SIP-запрос к серверу может быть повторен до 10 раз. Повторные запросы вместе с трафиком самой DDoS-атаки создадут дополнительную нагрузку на CSCF.

Повышенная нагрузка на CSCF ведет к тому, что не попавшие под атаку серверы других услуг не получают вовремя ответы от этого узла и также могут сгенерировать по 10 повторных запросов к нему в следующие 32 с, что вызовет полную перегрузку CSCF и отказ предоставления всех услуг.

Учитывая, что серверы услуг никогда не имеют десяти- или даже пятикратного запаса процессорной мощности, необходимой для выполнения логики услуг, видим, что для организации DDoS-атаки, которая способна нарушить работу IMS-сети, обслуживающей миллионы абонентов, злоумышленнику необходимо получить доступ всего к нескольким клиентским аккаунтам.

Примеры реализации фрода в IMS

Как уже отмечалось, уязвимости безопасности, затрудняющие обнаружение фрода в сетях NGN/IMS, порождаются двумя особенностями этих сетей, а именно: применением протоколов IP и SIP, а также разнообразием механизмов доступа. Как и в сетях ОКС7, в основанных на SIP сетях IMS маршруты передачи сигнальной и пользовательской информации разделены. Это также повышает вероятность нелегитимного пользования услугами.

Осуществлению многих видов фрода, например кражам и нелегитимному использованию IP-адресов, способствует открытость IP-сетей. Их децентрализованная архитектура предполагает наличие интеллектуальных пользовательских терминалов, способных напрямую контактировать с другими сетевыми элементами, что значительно увеличивает риск нелегитимного использования сетевых ресурсов.

Если терминалы пользователей подключены одновременно к сети IMS и публичному Интернету, то поль-

зователи получают возможность взаимодействовать непосредственно (peer-to-peer) с помощью прямой адресации, что может противоречить тарифной политике оператора сети IMS.

А вполне легитимная технология использования SIP-прокси-сервера в качестве учрежденческой АТС может применяться и для международного фрода путем разделения одного аккаунта между несколькими пользователями. В этом случае задействуется стандартная SIP-процедура переадресации, а группа пользователей работает с одним счетом, связанным с данным аккаунтом, что требует от оператора сети IMS, у которого зарегистрирован такой сервер, дополнительных мер контроля.

Предоставление услуг, основанных на IP-протоколе, зачастую связано с бизнес-моделью, отличной от модели ТфОП. В новой модели кроме потребителя и оператора сети участвуют и поставщик услуг, и поставщик контента, и оператор системы мобильных платежей. Любой их них может явиться целью фродстерской атаки, следовательно, для фрод-контроля необходимо собирать и сопоставлять данные от разных компаний, что намного его усложняет.

Фрод-сценарии зависят от услуг и технологий. С развитием NGN/IMS фрод продолжит эволюционировать, особенно с переходом от безлимитной «битовой трубы» к тарификации услуг на основе потребленного трафика и вида контента. Так, скорее всего, целью фродстеров станет не просто установление соединения, а скачивание дорогостоящего контента. Вместе с тем нельзя надеяться, что в эпоху NGN/IMS исчезнут традиционные, давно известные виды фрода.

Благодаря конвергентной природе сетей NGN/IMS угрозы различных видов (финансовые, исходящие из природы сети Интернет, от хакеров, от фродстеров) будут смешиваться/взаимно дополнять друг друга. Поэтому ранее самостоятельные подразделения противодействия фроду, управления рисками предприятия, гарантирования доходов и сетевой безопасности должны будут объединить свои усилия в борьбе с фродом.

Методы и системы противодействия DDoS-атакам и фроду в сетях NGN/IMS

Поскольку успешная DDoS-атака может привести к полной перегрузке серверов CSCF, механизм защиты целесообразно реализовывать в специализированном устройстве.

Идеально, если защита против подобных атак организована для каждого сетевого элемента IMS. Однако, учитывая требования к аппаратным компонентам, стоимость такого подхода может быть очень высока. Очевидный выход – акцентировать внимание на защите пограничных элементов IMS, таких как P-CSCF и A-BGF (Access Border Gateway Function), размещаемых на границе сети доступа между абонентскими терминалами и ядром сети, а также I-BCF и I-BGF (Interconnect Border gateway), находящихся на границе ядра сети с сетями других поставщиков услуг. Обычно функции системы обнаружения и предотвращения вторжений (IDPS) возлагаются на пограничный контроллер SBC (Session Border Controller), который формально не является частью инфраструктуры IMS.

Система IDPS предназначена для оперативного обнаружения начала DDoS-атаки и блокирования ее источника без прерывания предоставления услуг другим абонентам. Это требует оснащения SBC функциями мониторинга скорости сигнального потока, контроля форматов сообщений в комплексе с возможностью динамического создания «черного списка» IP-адресов источников атак.

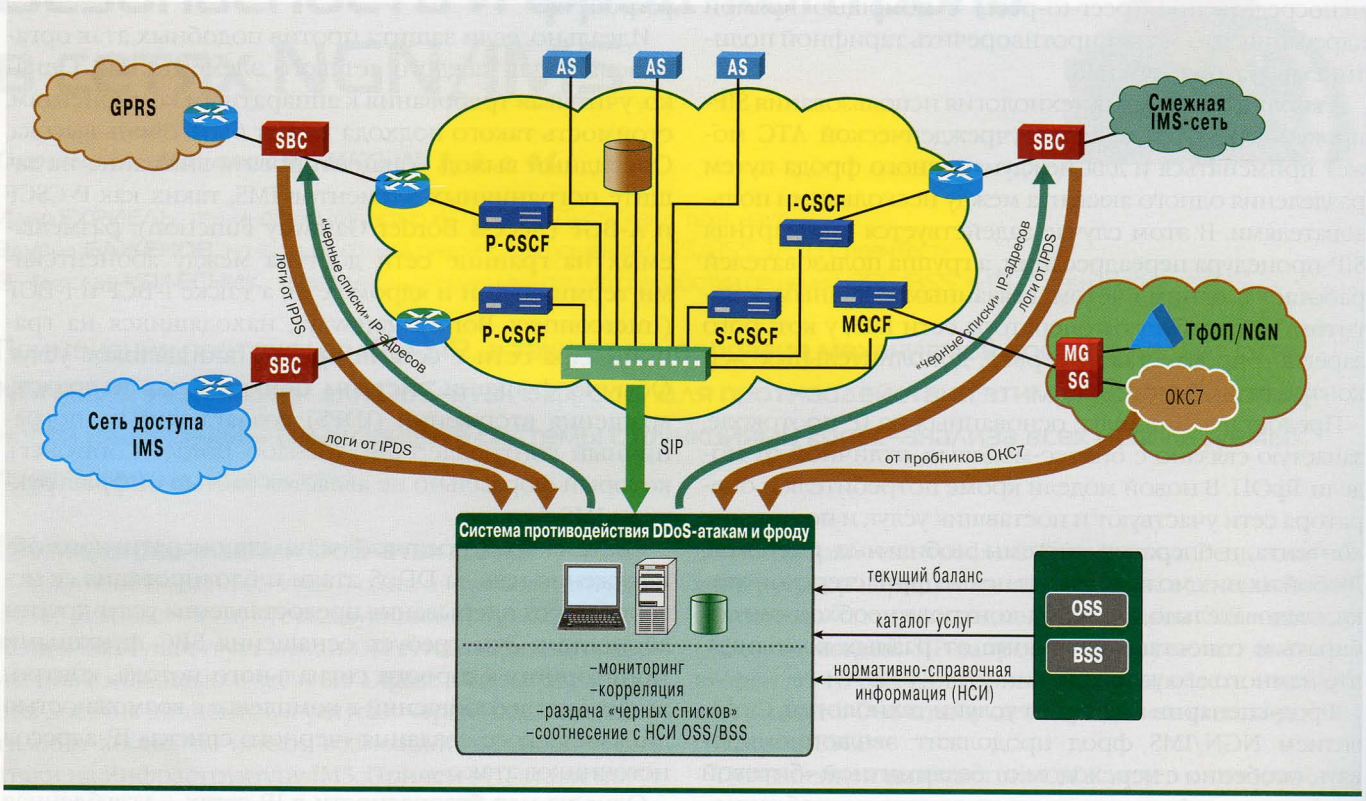
Одна из мер безопасности в IP-сетях – углубленная проверка пакетов (DPI), под которой подразумевается мониторинг и контроль пакетов на уровнях с второго по седьмой модели ISO/OSI.

Инспекция на нижних уровнях – с второго по четвертый – охватывает некоторые виды распознавания атак по типу DDoS, но не приводит к выявлению фрода.

Исследование уровней с четвертого по седьмой обычно входит в понятие «обработка контента». Именно здесь обнаруживаются многие виды угроз IMS: новейшие методы DDoS-атак с применением вредоносного ПО, спам, фишинг и нежелательный контент. Мониторинг и контроль однорангового трафика данных, в частности BitTorrent и LimeWire, также производится на этом уровне.

Системы анализа и противодействия фроду нужно оценивать не только по их способности локально анализировать характеристики сетевого трафика и противодействовать отдельным видам угроз, но и по способности сопоставлять множество факторов, влияю-

Пример организации системы противодействия атакам и фроду для IMS-сетей



щих на все аспекты безопасности процесса предоставления услуг.

В деле обеспечения безопасности мультисервисных услуг важен комплексный анализ угроз на всех участках технического обеспечения услуги. Это подразумевает выявление угроз не только на одном участке сети или для одного семейства протоколов, но и для их совокупности (SIP, ISUP, INAP, Sigtran, H.323/Megaco), поскольку в этом случае эффективность противодействия фроду значительно повышается.

Непосредственному осуществлению практически любого вида фрода предшествует DoS-атака, направленная на отказ одной из функций реализации логики услуги. Поэтому для результативной борьбы с фродом необходим совместный анализ логов от локальных систем IPDS, записей о сессиях IPDR, а также об объемах и структуре потребляемого трафика от пробов системы мониторинга.

Применение для борьбы с фродом только систем IPDS, даже оснащенных функциями DPI, не приводит к необходимому результату, поскольку они ориентированы на анализ сетевого трафика на локальном участке сети и вне контекста обеспечиваемой услуги. Контроллеры SBC не дают информации о характеристиках трафика клиента, который может косвенно влиять на IMS-услуги, и защищают на уровне протокола доставки сообщений, но не на уровне протокола, осуществляющего поддержку услуги.

С другой стороны, внедрение систем с функциями кросс-анализа и корреляции всех протоколов и подсистем, используемых для обеспечения услуги, сокращает время, необходимое для идентификации конкретного вида фрода и активации мер противодействия ему.

Система, способная обеспечить безопасность сети NGN/IMS, должна также выполнять контроль, распознавание и проверку контента на основе сигнатур с открытым набором правил. Сигнатуры позволяют классифицировать IP-трафик с помощью адресов IPv4 и IPv6, типов приложений, классов QoS и определяемых пользователем сигнатур приложений.

Кроме того, комплекс должен обладать программируемостью и дружественным интерфейсом пользователя для оперативной модификации и настройки встроенных средств исследования сложных текстовых протоколов, выявления вирусов и обнаружения вредоносных программ в полезной нагрузке.

■ ■ ■

Множество видов доступа, открытая распределенная архитектура, потенциальная одновременность DDoS-атак и фрода, широкая номенклатура новых услуг выдвигают ряд требований к системам противодействия атакам и фроду для IMS-сетей.

Некоторые уязвимости сетей IMS могут быть нивелированы на этапе проектирования сети, однако для достижения наилучшего результата безопасность должна быть обеспечена на всех уровнях архитектуры IMS специализированными системами. Основные требования к этим системам таковы: централизация контроля и сбор логов от локальных систем, возможность сопоставления информации о разных типах данных и протоколах, контроль контента, наличие встроенных шаблонов и гибкость настройки фрод-критериев. ИКС