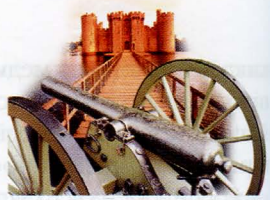
Безопасность и фрод-контроль в сетях NGN/IMS



IMS – Is Missing Security?*

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»

Архитектурную концепцию IMS, в рамках которой оператор может предоставлять абонентам разнообразные мультимедийные услуги, принято считать основой для построения NGN. Однако она имеет целый ряд уязвимостей, и над их «закрытием» надо серьезно работать.

Концепция IMS опирается на бизнес-модель, предполагающую, что оператор и поставщики услуг способны управлять доступом абонента к сети и услугам и начислять плату за их использование, исходя из вида услуги и объема ее потребления. Это в корне отличается от принятой в Интернете модели, при которой сеть оператора служит «битовой трубой», а поставщик услуг предлагает безлимитные тарифы.

Но, как это часто бывает, с новыми рыночными возможностями сопряжены дополнительные риски. Так, в результате перехода к основанной на протоколе IP открытой архитектуре операторы встретились с новыми угрозами безопасности, напрямую влияющими на их бизнес. Эти угрозы можно разделить на два вида:

- технические угрозы, связанные с открытыми стандартами и проявляющиеся на всех уровнях архитектуры IMS;
- направленные как на оператора, так и на абонентов попытки нелегитимного использования услуг и/или кражи конфиденциальной информации.

Поскольку оборудование, входящее в состав IMS-платформ, имеет уязвимости, присущие любым основанным на IP-протоколе решениям, и следовательно, подвержено атакам червей и вирусов, DDoS, спаму и различным видам фрода, то, применяя концепцию IMS для развертывания сетей нового поколения, на обеспе-

*IMS – это потерянная безопасность? (англ.).

Архитектура IMS

Как известно, разработанная консорциумом 3GPP архитектура IMS представляет собой сеть, наложенную поверх сети IP. Для сигнализации используется протокол SIP. В IMS выделяются четыре функциональных уровня:

- уровень приложений услуг (содержит IMS-приложения);
- уровень управления (выполняет функции управления доступом к приложениям с помощью протокола SIP, администрирования пользователей и услуг, биллинга и др.);
- транспортный уровень (обеспечивает внутри- и межсетевую связность);
- уровень доступа (предоставляет доступ к абонентской сети, например, для DSL-модемов или 3G-телефонов).

Хотя в процессе предоставления мультимедийных услуг в IMS используется много протоколов (HTTP, SMTP, Diameter и др.), роль основного протокола управления играет SIP. Выбор SIP обусловлен наличием в нем легкого и открытого метода установления связи со сложными мультимедийными приложениями и управления ими во время сессии в IP-сетях.

В центре архитектуры IMS (см. рисунок) находится функциональный элемент CSCF (Call Session Control Function) – основной SIP-сервер, который может относиться к одному из трех типов. Прокси P-CSCF (Proxy CSCF) создает внешний интерфейс с терминалами пользователей при их первом контакте с IMS; обслуживающий S-CSCF (Serving CSCF) принимает вызов на обслуживание, а I-CSCF (Interrogating CSCF) обеспечивает внешний интерфейс с другими IMS-сетями.

Узел HSS (Home Subscriber Server) содержит базу данных реквизитов клиентов, идентифицирует домашний S-CSCF, а также участвует в аутентификации пользователей и проверке их прав доступа к определенным услугам.

Абоненты сотовых сетей получают доступ к IMS через узел GGSN (Gateway GPRS Support Node), который для IMS выполняет функции маршрутизатора, проключающего клиентов через сеть IP. Обратиться к IMS можно и через сеть Wi-Fi, а также с помощью проводных IP-устройств. Соединение с ТфОП выполняется через медиашлюзы, которые управляются узлом MGCF (Media Gateway Control Function).

Новые услуги развертываются в инфраструктуре IMS в виде SIP-серверов приложений (SIP-AS). Доступ к серверам приложений

чение их безопасности необходимо обращать самое серьезное внимание.

Уязвимые точки IMS

Главные причины повышенной уязвимости сетей NGN/IMS – распределенность и открытость архитектуры, использование протокола SIP в качестве управляющего и множественность видов доступа.

Поскольку основа любой IP-сети достаточно проста (протоколы IP, TCP и UDP), то при реализации мультимедийных услуг именно сложный протокол SIP и приложения оконечных устройств обеспечивают большинство функций системы IMS.

А в оконечных устройствах значительная часть функций системы может управляться пользователями. Помимо этого, заголовки протокола SIP – текстовые и открыты для изменений. Из-за этого возможны различные виды перехвата сессии и регистрации, когда злоумышленник изменяет параметры заголовка SIP и перехватывает контроль над соединением.

Последствия атак, проведенных непосредственно на уровне SIP, как правило, серьезные: могут осуществляться подмена идентификации, перенаправление вызовов и получение идентификационных данных.

Рядовой пользователь не имеет необходимых технических средств и недостаточно технически грамотен, чтобы самостоятельно проверить, насколько его технология доступа соответствует стандартам безопасности. Более того, большинство пользователей не знают, какая технология доступа на самом деле применена. Провайдер услуг NGN/IMS зачастую также не имеет возможности определить безопасность сценария доступа каждого пользователя.

Основные угрозы сетям NGN/IMS и требования к обеспечению их безопасности

Список угроз безопасности IP-сетям следующего поколения и их абонентам известен. В него входят атаки типа «отказ в обслуживании» (DoS/DDoS), непредумышленные перегрузки трафиком (spoofing), вирусы и черви, фрод, кража идентификационных данных, спам по Интернету (SPIT).

Рабочая группа консорциума 3GPP, которая отвечает за анализ новых угроз безопасности, вызванных IP-услугами и системами, выработала требования к обеспечению безопасности в сетях IMS и установила, что ее уровень должен быть по крайней мере не ниже, чем в GSM-системах второго поколения.

По понятной причине внимание этой рабочей группы ограничивается анализом и разработкой требований безопасности к архитектуре IMS для сетей 3G. В частности, она указала на необходимость защиты SIP-сигнализации между абонентским терминалом и ядром IMS и применения аутентификации абонентов, не специфицируя при этом механизмы авторизации доступа к ядру IMS абонентов со стороны сетей фиксированной связи. Однако некоторые особенности системы IMS, важные для снижения рисков безопасности, требованиями 3GPP не охватываются вовсе, а некоторые охватываются лишь частично (см. таблицу).

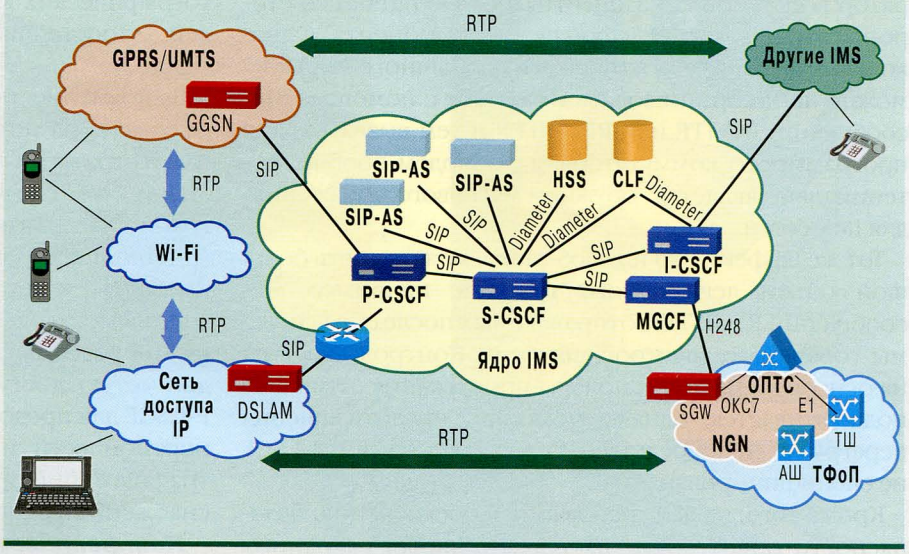
Требования безопасности к системе IMS должны включать в себя скрытие топологии на интерконнект-

осуществляется посредством SIP-сообщений, направляемых от S-CSCF к нужному SIP-AS на основании специальным образом сконфигурированных триггеров, идентифицирующих запросы к определенной услуге. Сервер SIP-AS, реализующий какую-либо услугу, например услугу присутствия, может использоваться и другими услугами, если в их алгоритм входит поддержка соответствующей этому серверу функции.

Таким образом, архитектура IMS позволяет оператору развертывать сложные мультимедийные услуги, однако в ней есть множество интерфейсных точек, безопасность обмена информацией в которых необходимо контролировать.

Стандарты допускают как реализацию всех функциональных элементов архитектуры IMS в виде одного аппаратно-программного

Архитектура IMS



устройства, так и выделение их в отдельные устройства. Конкретное решение зависит от сложности развертывания, стоимости, масштабируемости и требований к обеспечению безопасности.

Соответствие требований безопасности и видов угроз для сетей NGN/IMS

Требования к обеспечению безопасности инфраструктуры IMS	Поддержка требований функциями IMS	Угрозы безопасности					
		DoS/DDoS	Перегрузка трафиком	Вирусы	Фрод	Кража идент. данных	SPIT
Контроль доступа к статическим IP-адресам	Да	■	■	■			
Контроль доступа к динамическим IP-адресам	Нет	■	■	■	■		
Скрытие топологии, NAPT на 3 и 5 уровнях	Частично	■	■	■			
Авторизация абонента и CSCF	Да, IPsec, SIP Digest	■	■	■	■	■	■
Авторизация абонента	Да, HSS				■	■	■
Шифрование сигнализации	Да, IPsec					■	
Контроль доступа к ресурсам в I/S-CSCF	Нет		■				
Контроль доступа к полосе пропускания сети	Да, PDF/RACF		■				
Ограничение числа сессий для пользователя	Нет				■		■
Ограничение полосы пропускания для пользователя	Нет				■		
Проверка содержимого сообщений SIP и аттачментов MIME	Нет			■		■	
Контроль интенсивности сигнальных сообщений	Нет	■	■				
Контроль используемой полосы пропускания	Нет	■	■		■		
Ограничение числа вызовов	Нет		■				■
Управление маркированием/ соотнесением QoS	Нет				■		

Обозначения:
- ■ – требование выполняется некоей функцией, определенной стандартами IMS;
- ■ – функциональность стандартами не определена;
- ■ – функциональность определена частично;
- ■ – выполнение требования существенно влияет на предотвращение соответствующей угрозы;
- □ – выполнение требования на предотвращение угрозы не влияет.

границах, аутентификацию и авторизацию абонентов, шифрование сигнализационного обмена и контроль доступа на основе имеющейся полосы пропускания сети.

Между тем в текущей версии стандарта функция NAT определена только на границе взаимодействия с внешними сетями, в предположении, что на границе с сетью доступа скрытие топологии не понадобится, а оператор всегда сможет защититься от DoS-атаки со стороны мобильного телефона своего абонента. Однако на практике уже доказано, что с обычного ноутбука можно легко организовать DoS-атаку с помощью SIP-сообщений INVITE или REGISTER и тем вызвать отказ программного коммутатора, а 3G-модем вообще потенциально является «оружием массового поражения» для IMS-сетей.

Тот же эффект, что и DDoS-атака, может иметь большой объем легитимного трафика, например SIP-сообщений REGISTER, отправляемых после сбоя системы городского электроснабжения. Контроль доступа на основе имеющейся полосы пропускания сети в IMS поддерживается, однако механизм предотвращения перегрузки непосредственно в узлах S-CSCF и I-CSCF не специфицирован.

Кроме того, не все требования к обеспечению безопасности операторам удается выполнить на ранних этапах развертывания IMS. Так, хотя протокол IPv6 для IMS специфицирован, реальное внедрение происходит в условиях инфраструктуры IPv4, а существующие пользовательские терминалы, например мобильные телефоны, не поддерживают IPsec.

Учитывая реалии переходного периода, консорциум 3GPP утвердил стандарт для ранних реализаций IMS, в котором требования к безопасности несколько снижены. Например, для проводных IP-устройств пользователю разрешается использовать пароль вместо криптографических ключей, а как известно, подбор паролей – простейший способ начала реализации любых угроз.

Выполнение необязательных для IMS требований оставлено на усмотрение производителей оборудования и стратегий внедрения.

При этом следует принимать во внимание, что пограничные сигнальные элементы P-CSCF и I-BCF (Interconnect Border Gateway Function) обеспечивают доступ к сети IMS с точки зрения безопасности. Эти элементы лучше физически отделить от S-CSCF и I-CSCF, размещенных в центре IMS. На границе с каждой сетью доступа целесообразно иметь несколько P-CSCF для предотвращения DDoS-атак на ядро транспортной сети и минимизации влияния перегрузок трафиком при рестарте системы после отказа энергоснабжения в одном из районов города.

Конкретные примеры организации DDoS-атак и фрода в сетях NGN/IMS, а также методы противодействия им – в следующем номере «ИКС».