Эссе по курсу "Защита информации", кафедра радиотехники,
Московский физико-технический институт (ГУ МФТИ),
http://www.re.mipt.ru/infsec

Безопасность в мобильных сетях 3го поколения: угрозы, возникающие при передаче данных через IP

Подворчан Николай

05 апреля 2007 года

г. Долгопрудный

В 21 веке операторам мобильной связи необходимо осознать свою роль в качестве поставщиков Интернет-услуг. В настоящее время они оказывают не только услуги передачи голоса, то также и обеспечивают пользователей высокоскоростными сервисами на базе IP-протокола. Таким образом, для того чтобы иметь возможность предложить клиентам более широкий спектр услуг и более богатый выбор мобильного контента, операторы открывают доступ к своим ранее закрытым сетям большому числу других мобильных операторов, сетям передачи данных и публичному Интернету.

В результате, 3G сети теперь подвержены не только уже хорошо известным уязвимостям, но также и характерным только для мобильной области вирусам и троянам, и, кроме того, могут пасть жертвой непосредственных атак, таких, например, как Denial of Service (DoS) (отказ в обслуживании), со стороны хакеров или преступных группировок. С этим типом атак давно знакомы "кабельные" Интернет-провайдеры. Существует несколько разновидностей упомянутых атак, которые используют слабые места в архитектуре и некоторых протоколах, применяемых в сотовых сетях поколений 2.5G/3G.

Примеры атак

Нелегальный доступ к информации об абонентах

Эти типы атак на сети мобильных операторов происходят достаточно часто, и понятно, что будут происходить в дальнейшем. Сейчас уже можно с лёгкостью найти в продаже базы данных российских операторов сотовой связи, да и США прославились громким скандалом в 2004 году, когда произошла значительная утечка данных абонентов T-Mobile.

Очевидно, что невнимание к данному вопросу может сказаться не только на доходах операторов, то также и на их клиентах, персональные данные которых вполне могут стать доступны заинтересованным лицам.

Атаки Denial of Service

Данный тип атак на сеть также вполне вероятен. К примеру, в 2005 году, учёные из Penn State University опубликовали доклад, в котором подробно описали, каким образом SMS, отправляемые из Интернета, могут быть использованы для перегрузки SMS-центра оператора, и потенциально, для перегрузки сети вообще.

Также DoS возможно провести, непосредственно действуя на радиоспектр, создавая помехи в заданной области частот.

Распространение вирусов

Недавно вышедшая статья Лаборатории Касперского описывает интересный случай быстрого распространения вируса для мобильных аппаратов Cabir, который произошёл в Хельсинки в августе 2005 года, во время Чемпионата Мира по лёгкой атлетике. Cabir тогда передавался из аппарата в аппарат во время передачи данных через Bluetooth. Пользователи, не задумываясь, принимали запросы на передачу файлов и таким образом заражали свои телефоны. Если бы эта вспышка не была во время остановлена, Cabir имел бы возможность проникнуть в миллионы аппаратов по всему миру.

Этот пример показывает, с какой лёгкостью может распространяться вирус. А ведь если всего-навсего перевести Bluetooth-соединение в состояние 'hidden', то это остановит передачу червя. Другие типы мобильных вирусов и червей, такие как ComWar, могут распространяться через MMS - и именно эту разновидность распространения Лаборатория Касперского считает наиболее опасной, т.к. вредоносные программы могут быть переданы на любое расстояние. И т.к. MMS также отправляются на e-mail адреса, то этот сервис может служить гейтом при распространении вирусов с ПК на мобильные аппараты и обратно.

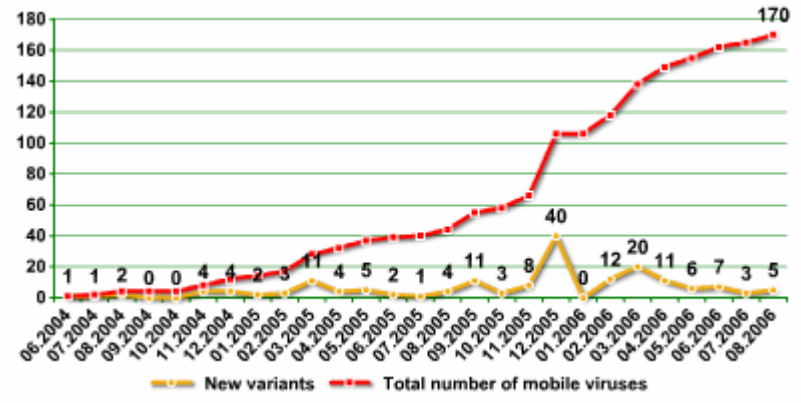

Рис. 1. Рост количества разновидностей известного мобильного вредоносного ПО.

Источник:
Лаборатория Касперского, 2006

Типы атак, характерные для 3G

По мере того как операторы переходят к оказанию 3G услуг, они, в большинстве своём, не строят сеть с нуля, а вместо этого модернизируют существующую инфраструктуру 2.5G сетей: GSM/GPRS/EDGE или CDMA/CDMA 1X. Например, большая часть базовых станций UMTS может быть расположена на площадках уже существующих БС GSM, а сама сеть GSM/GPRS может стать основой для сети 3G. При этом нужно усовершенствовать узел поддержки GPRS (SCGN), но центры мобильной коммутации (MSC) требуют только минимальной модернизации, а шлюзовой узел GPRS (GGSN) вообще может не обновляться.

Именно из-за того, что 3G сети зачастую представляют собой апгрейд сетей 2.5G, в них изначально не заложены принципы безопасной передачи IP-данных. Более того, IP-область является относительно новой для операторов, ведь раньше они имели дело лишь с защитой передачи голосовых данных.

Все виды атак на мобильные сети можно условно разделить на две категории:

- *Внешние*: из Интернета, частных сетей, сетей других операторов.
- *Внутренние*: от мобильных устройств, таких как смартфоны, коммуникаторы, ноутбоки и даже персональные компьютеры, подключенные к сети 3G.

В таблице 1 приведены типы атак, которым сейчас подвергаются мобильные операторы:

Тип атаки	Атакуемые элементы сети	Цель атакующего
Черви, вирусы, трояны, спам посредством SMS/MMS	Другие пользователи сети, сервера с мобильным контентом	"Интерес", отказ в обслуживании (DoS), перерывы в работе сети.
DoS, SYNflood, атаки на уровне приложений (на сервера RADIUS, переполнение буфера, RTP flooding, и т.д.)	HLR, AAA, сервера с контентом, модуль обработки вызовов (signalling node)	Сделать невозможной работу сети
Overbilling attack	Элементы управления сетью (AAA, HLR, VLR, и т.д.)	Мошенничество
Подделка PDP контекста	User-sessions	Нелегальное получение доступа к услугам
Атаки на сигнальном уровне (SIGTRAN, SIP)	Signaling nodes	Сделать невозможной работу сети

Denial of Service

На данный момент одной из самых преобладающих угроз для кабельных Интернет-провайдеров является распределённая атака на отказ в обслуживании (Distributed Denial of Service, DDoS). По существу, атаки DDoS используют "brute force" методы, для того чтобы переполнить атакуемую систему входящими данными с целью замедления её работы или остановки вообще. Создание достаточного количества трафика для достижения вышеупомянутой цели требует наличия сети взаимодействующих компьютеров, которые часто называют "ботами". Лэптопы, смартфоны, блэкберри, PDA, подключенные к Интернету через широкополосное соединение, вполне могут играть роль таких "ботов".

Overbilling attacks

Другой тип атаки называют "овербиллингом". Овербиллинг заключается в том, что нелегальный пользователь похищает IP-адрес абонента и затем использует установленное соединение для скачивания платного контента, либо просто использует его в своих личных целях. В любом случае, легальному пользователю предъявляется счёт за трафик или контент, которые он никогда не заказывал.

Подделка PDP контекста

Этот тип атак использует уязвимость в GTP (GPRS Tunneling Protocol). Их действие может проявиться следующим образом:

- Фальшивые пакеты "delete PDP context" могут вызвать потерю соединения у конечного пользователя
- Фальшивые пакеты "create PDP context" могут повлечь за собой неавторизованный или вообще нелегальный доступ к Интернету или сетям клиентов.
- Большое число поддельных пакетов GTP является типом Denial of Service.

Более подробно о GTP будет рассказано ниже в секции "*Сигнальный протокол GTP*"

Атаки на сигнальном уровне

SIP (Session Initiation Protocol) - это сигнальный протокол, используемый в IMS-сетях для оказания услуг *Voice over IP (VoIP).* Существует несколько хорошо известных уязвимостей у VoIP-систем, основанных на SIP. К примеру, у функции *Call Manager* (отвечающая за роутинг звонков и сигнальный трафик в VoIP системах) есть бреши, которые могут позволить хакерам сделать следующее:

- Изменить установки VoIP и получить доступ к информации об аккаунтах отдельных пользователей
- Подслушать разговоры через VoIP
- Похитить данные VoIP пользователя и пользоваться услугой за его счёт.

Уязвимые узлы сетей

По большому счёту, в сетях мобильных операторов существует большое число уязвимых точек:

- Само мобильное оборудование, т.е. ноутбуки, сотовые телефоны, коммуникаторы, смартфоны
- Радиолинк между мобильным аппаратом и сотовой базовой станцией - это соединение UMTS/HSDPA или EV-DO
- Интерфейсы к другим мобильным сетям - в сетях GPRS/UMTS это интерфейс Gp
- Интерфейсы к сетям передачи данных - Интернету или частным сетям; в GPRS/UMTS сетях за это отвечает интерфейс Gi.
- Элементы управления и технические модули, такие как Home Location Register (HLR), который хранит данные об абоненте (интерфейс Ga в сети GPRS/UMTS).
- Сервера приложений (application servers) и сервера с контентом (content servers)
- Между- и внутрисетевые сигнальные протоколы и интерфейсы.

Можно сказать, что в мобильных сетях с "внешним миром" взаимодействуют два основных элемента: GGSN в сетях GPRS/EDGE/UMTS и Packet Data Serving Node (PDSN) в CDMA 1x/EV-DO. Если рассмотреть в качестве примера UMTS, то абонент выходит в Интернет через SGSN, соединённый посредством GTP с GGSN. На рисунке 2 изображена структура этого типа сети.

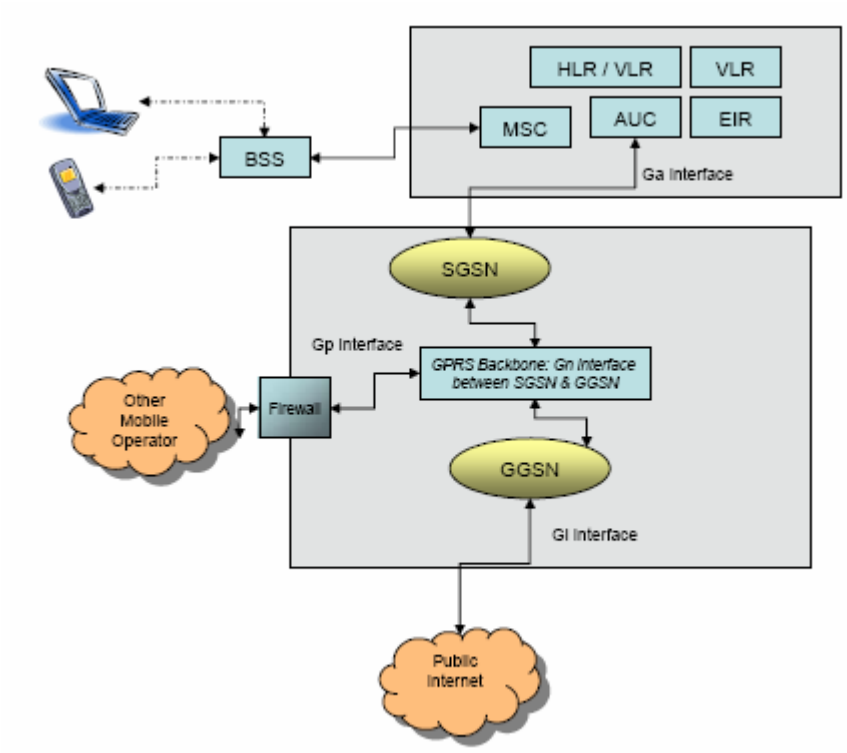

Рис. 2. Структура GPRS/UMTS сети

Источник:
iGillotResearch, 2006

Сигнальный протокол GTP

Остановимся подробнее на этом моменте. Для сигнализации и туннелирования между GGSN и SGSN используется, как уже упоминалось выше, протокол GTP. SGSN использует GTP для активации сессии по запросу абонента - это называют "активацией PDP контекста". PDP контекст есть структура данных, содержащая такую информацию, как временный IP-адрес пользователя, идентификаторы сессии GTP (GGSN и IMSI (International Moblile Subscriber Identity)).

Однако, GTP не поддерживает аутентификацию, проверку целостности данных и защиту конфиденциальности, чем могут воспользоваться хакеры. Именно это делает GTP одной из самых уязвимых точек в сетях GPRS/UMTS.

Обеспечение безопасности

Остановимся теперь на технологиях, которые обеспечивают защиту от вышеперечисленных атак. Мобильным операторам, как упоминалось в начале, для отражения атак на свои сети необходимо относиться к себе именно как к провайдерам Интернет-услуг. Это подразумевает разработку многоуровневой системы защиты, которая:

- Должна строиться с учётом особенностей новых разновидностей атак
- Концентрирует, где это только возможно, обработку данных в малом числе дата-центров. Многие операторы Европы уже сделали этот шаг в направлении более надёжной защиты своих сетей.
- Обеспечивает безопасность конечных пользователей путём внедрения новых технологий и ПО - такого как антивирусы, файрволы, и т.д. Это позволяет покрыть проблемы защиты на файловом уровне.
- Заключается также во внедрении файрволов, VPN и IDP-систем в соответвующие "слабые звенья" сети, что обеспечивает защиту на сетевом, сессионном уровнях и уровне приложений.

Тип атаки	Атакуемые элементы сети	Способы защиты
Черви, вирусы, трояны, спам посредством SMS/MMS	Другие пользователи сети, сервера с мобильным контентом	Антивирусное ПО, проверка контента на безопасность
DoS, SYNflood, атаки на уровне приложений (на сервера RADIUS, переполнение буфера, RTP flooding, и т.д.)	HLR, AAA, сервера с контентом, модуль обработки вызовов (signalling node)	Файрволы уровня приложений, сигнального уровня, IDP
Overbilling attack	Элементы управления сетью (AAA, HLR, VLR, и т.д.)	IDP
Подделка PDP контекста	User-sessions	Файрволы сигнального уровня
Атаки на сигнальном уровне (SIGTRAN, SIP)	Signaling nodes	Файрволы уровня приложений, сигнального уровня, IDP

Если с защитой от вирусов, троянов и прочего вредоносного ПО ситуация в общем ясна -- необходимо обеспечивать защитным программным обеспечением абонентов, а также внедрять его непосредственно в центрах обработки данных --, то с другими видами атак ситуация не так очевидна. Рассмотрим их подробнее.

Файрволы и IDP

При разработке и внедрении систем безопасности, обычно выделяют три уровня защиты:

- *Уровень пакетов*. На нём могут действовать stateless-файрволы, определяющие валидность пакета путём анализа основной информации из его заголовка.
- *Сессионный уровень*. Субъектами данного уровня можно считать stateful-файрволы, которые контролируют поток трафика между сетями, отслеживая состояние сессии и отбрасывая пакеты, не являющиеся частью авторизованной сессии.
- *Уровень приложений*. На этом уровне функционируюи системы IDP, которые анализируют сетевой трафик на признаки атак.

Рисунок 3 иллюстрирует сказанное выше.

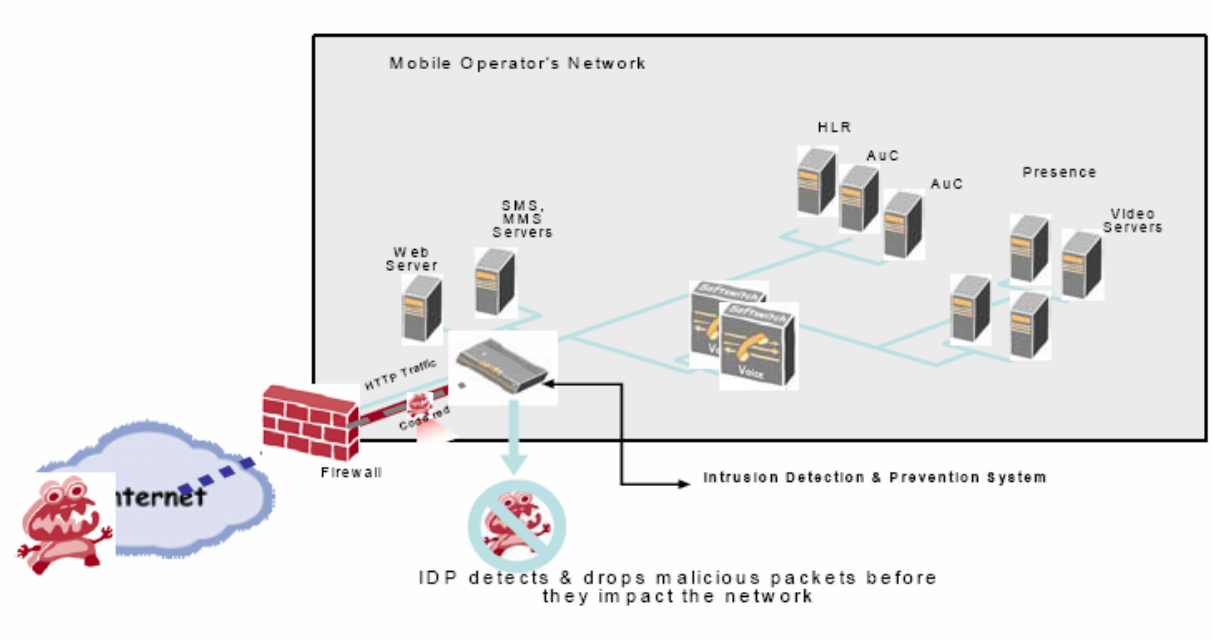

Рис. 3. Иллюстрация работы файрволов и IDP. Источник: *Jupiner Networks, 2006*

Защита GTP

Как изображено на рисунке 4, уязвимость GTP возможно преодолеть, передавая данные посредством технологии IPSec VPN, а также устанавливая файрволы, которые будут отсекать трафик, предназначавшийся для использования слабых мест GTP. И так как GGSN соединяет сеть GPRS/UMTS с внешними сетями, то она подвержена всем типам атак, которые могут предприниматься в отношении этих сетей. Существует несколько различных взаимодополняющих друг друга способов обеспечить стойкость GGSN по отношению к атакам, таких как, например, установка файрвола с возможностями IDP на канал соединения с Интернетом.

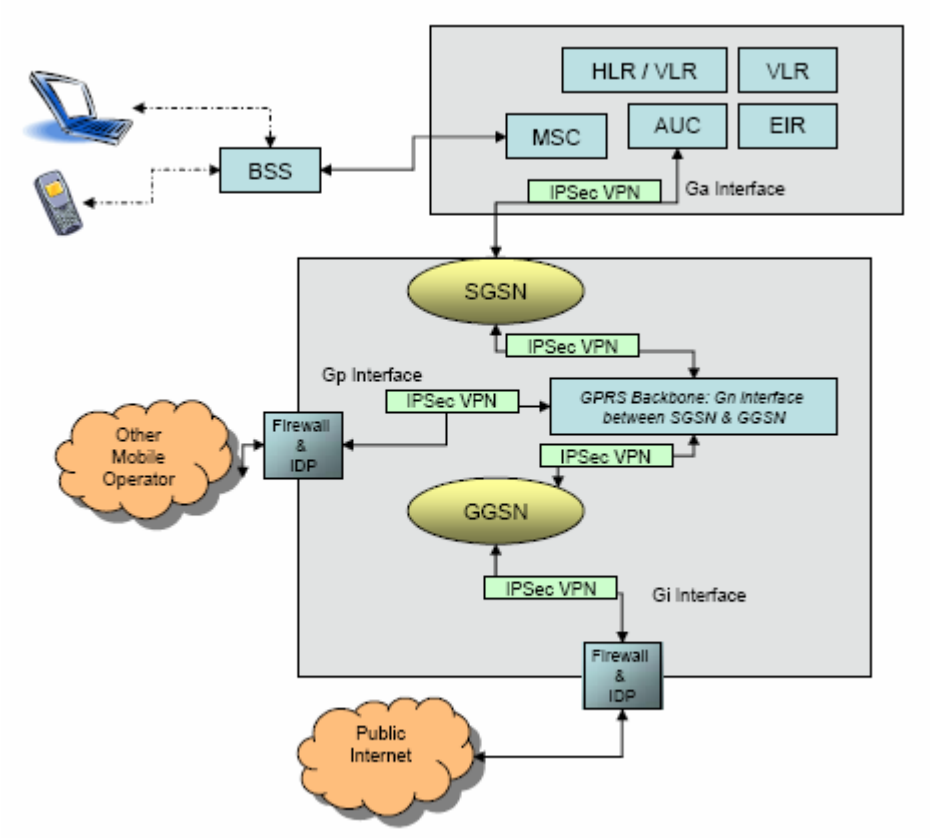

рис. 4. Использование VPN в сетях GPRS/UMTS

Источник: *iGillotResearch, 2006*

Выводы

Фантазия и возможности взломщиков сети не ограничены практически ничем. Для своих целей они могут применять: DoS атаки с участием т.н. "ботов", вредоносное ПО, а также атаки, использующие незащищённые места в сигнальных протоколах, таких как GTP, которые являются состаляющей многих сетей сотовой связи. Операторы должны умело противостоять этому. Также им всегда необходимо быть начеку, быть готовыми к появлению новых разновидностей атак, которые на данный момент могут даже казаться неосуществимыми…

Литература

1. 3G Mobile Network Security, *iGillotResearch*, January 2007. http://www.telecommagazine.com/
2. Mobile Malware Evolution: An Overview, Part 1. *Alexander Gostev, Kaspersky Lab* (http://www.viruslist.com/en/analysis?pubid=200119916)
3. Знакомимся с Session Initiation Protocol. *Кирен Маккорри* (http://www.osp.ru/win2000/2003/01/175733/)
4. О Radius подробно. *Роберт Шотт* (http://www.osp.ru/lan/2003/01/137078/)
5. GSM core network. *Портал "Википедия"* (http://ru.wikipedia.org/wiki/EIR#EIR)