**Безопасность технологии GPRS**

Алексей Лукацкий

GPRS (General Packet Radio Service) - это новая перспективная технология, стандартизация которой началась в 1993 году в European Telecommunication Standards Institute (http://www.etsi.org/), позволяющая работать в сети Internet, используя обычный мобильный телефон. С помощью GPRS, пользователи могут работать со своей электронной почтой, с обычными Web-серверами (а не со специальными WAP-версиями) и т.д. Основное достоинство GPRS-сетей состоит в том, что пользователь оплачивает только объем передаваемой/получаемой информации, а не время нахождения в сети. До разработки технологии GPRS (http://www.gsmworld.com/technology/gprs/index.shtml), абонент оплачивал все время соединения независимо от того, использовал он установленный канал передачи данных. Иными словами, ресурсы сети задействованы только во время непосредственной передачи данных от телефона. Во время пауз (например, просмотр полученной электронной почты) ресурсы сети предоставляются в распоряжение других абонентов. Кроме того, технология GPRS является промежуточным этапом при переходе от сетей 2 поколения (GSM) к 3-му (UMTS). В GPRS максимально возможная скорость передачи данных составляет 171,2 Кбит/с - это почти в 12 раз быстрее работы передачи данных в обычных сетях GSM (9,6 Кбит/с). Однако на данный момент скорости не так высоки - обычно 30-40 Кбит/с. В настоящее время три крупнейших сотовых сети России (МТС, БиЛайн, Мегафон) предлагают своим абонентам услуги GPRS. Потенциальное число абонентов технологии GPRS в России - 17,8 миллионов человек, именно такое количество абонентов сотовой связи насчитывалось в России к концу 2002 года. Реальное же число желающих воспользоваться преимуществами этой технологии пока не так велико. В частности, к началу декабря 2002 года в БиЛайне, пионере GPRS в России, насчитывалось всего 25000 абонентов.

**Архитектура GPRS**

Если не вдаваться в глубокие технические подробности, то технология работы GPRS выглядит следующим образом. Архитектура GPRS расширяет стандартные компоненты GSM новыми или обновленными элементами. В целом, таких элементов всего 4, из которых только 2 не были известны в технологии GSM.

**Мобильная станция**

MS (mobile station) - это мобильная станция, в качестве которой может выступать переносной или карманный компьютер, мобильный телефон или иное устройство, поддерживающее технологию GPRS. Функционально данный элемент состоит из 2-х компонентов, которые могут быть выполнены как в виде единого устройства (например, мобильный телефон Sony Ericsson T68i), так и в виде самостоятельных устройств:

терминальное оборудование (terminal equipment, TE), например, переносной компьютер;

мобильный терминал (mobile terminal, MT), например, модем.

В зависимости от типа оборудования и возможностей сети данная станция может работать в одном из 3-х режимов работы:

Класс A - позволяет мобильной станции в одно и то же время передавать как данные, так и голос, т.е. одновременно работать в GSM- и GPRS-сетях.

Класс B - позволяет мобильной станции передавать и данные и голос, но в разные моменты времени, т.е. не одновременно.

Класс C - позволяет мобильной станции работать только в режиме GPRS.

При подключении к сети GPRS, мобильная станция (а точнее элемент TE) получает IP-адрес, который не меняется до момента отключения мобильного терминала (MT); больше того, мобильная станция может даже и не "подозревать" о том, что она является мобильной. Мобильная станция устанавливает соединение с узлом обслуживания абонентов GPRS, описываемым далее.

**Базовая станция**

BSS (base station system) - это базовая станция, которая принимает радиосигнал от мобильной станции и, в зависимости от того, что передается (голос или данные), транслирует трафик:

на центр коммутации (mobile switching center, MSC), являющийся стандартным элементом сети GSM, или на узел SGSN, отвечающий за обработку входящих/исходящих данных GPRS.

Узел обслуживания абонентов GPRS

Обслуживающий узел (serving GPRS support node, SGSN) является основным компонентом GPRS-сети. Он транслирует IP-пакеты, посылаемые/получаемые мобильной станцией. По своей сути, это такой же центр коммутации, как и MSC в GSM, но в отличие от последнего, он коммутирует пакеты, а не каналы. Как правило, такой узел построен на базе ОС Unix и имеет свой IP-адрес. С точки зрения безопасности, на SGSN возложены функции:

Проверки разрешений абонентов на пользование запрашиваемых услуг (аутентификация). Механизм аутентификации GPRS совпадает с аналогичным механизмом в GSM.

Мониторинг активных абонентов.

Регистрация новых абонентов.

Шифрование данных. Алгоритм шифрования в технологии GPRS (GEA1, GEA2, GEA3) отличаются от алгоритмов шифрования в GSM (A5/1, A5/2, A5/3), но разработаны на их основе.

**Узел маршрутизации GPRS**

Узел маршрутизации (gateway GPRS support node, GGSN), также является важнейшим элементом технологии GPRS и отвечает за прием/передачу данных из внешних сетей, например, Internet или GPRS-сети другого оператора связи. С точки зрения внешней сети GGSN - это обычный маршрутизатор (как и SGSN, построенный на базе Unix), который принимает данные для всех подписчиков услуг GPRS. Помимо маршрутизации, GGSN отвечает за выдачу IP-адресов и тарификацию услуг.

Другие элементы GPRS-сети

Home Location Register (HLR) - это реестр собственных абонентов сети, которая хранит информацию о каждом человеке, оплатившем услуги оператора GPRS именно данной сети. В частности, HLR хранит информацию о дополнительных услугах, параметрах аутентификации, IP-адресе и т.д. Обмен данной информацией происходит между HLR и SGSN.

Visitor Location Register (VLR) - это реестр перемещений, которая хранит информацию о каждой мобильной станции, находящейся в данный момент в зоне действия SGSN. В VLR хранится та же информация об абоненте, что и в HLR, но только до тех пор, пока абонент не покинет географическую зону, обслуживаемую этим реестром перемещений.

Equipment Identity Register (EIR) - это реестр идентификационных данных оборудования, который содержит информацию, позволяющую блокировать вызовы от украденных, мошеннических или иных неавторизованных устройств.

Механизмы безопасности GPRS

Если посмотреть внимание на рис.1, то можно выделить следующие фрагменты GPRS-сети, на безопасность которых необходимо обратить соответствующее внимание:

безопасность мобильной станции безопасность соединения между мобильной станцией и узлом обслуживания SGSN безопасность данных в процессе их передачи по сети GPRS безопасность данных в процессе их передачи между различными операторами GPRS-услуг безопасность данных в процессе их передачи в сети открытого доступа, например, Internet.

**Безопасность мобильной станции**

Наибольший интерес вызывает безопасность мобильного телефона, который в терминах GPRS является мобильной станцией. Его безопасность складывается из двух составляющих:

SIM-карта сам телефон

SIM-карта (Subscriber Identity Module) - это модуль идентификации абонента. В SIM-карте содержится информация о сервисах, предоставляемых абоненту, независимая от типа используемого мобильного оборудования. Эта карта может вставляться в любой другой GSM терминал, при этом абонент получает возможность использовать этот терминал для получения всех сервисов системы, на которые он подписан. С точки зрения безопасности SIM-карта отвечает за идентификацию абонента и аутентификацию мобильного телефона в GPRS-сети. Она содержит идентификатор IMSI, индивидуальный ключ аутентификации абонента длиной 128 бит Ki, алгоритм генерации ключей шифрования A8 и алгоритм аутентификации A3 и разумеется PIN-код для доступа к функциям карты. Алгоритм A5 наряду с IMEI включен в состав программного обеспечения телефона и обеспечивает его защиту.

Каждый абонент в GPRS-сети имеет уникальный международный идентификатор мобильного абонента (IMSI, International Mobile Subscriber Identity), хранимый в SIM-карте. IMSI состоит из 3 элементов:

трехразрядный код страны (для России - 250) двухразрядный код сети (для МТС - 01, для Билайн - 99, для СМАРТС - 07 и т.д.) десятиразрядный код абонента (Mobile Subscriber Identity Number, MSIN).

Алгоритм A8 отвечает за генерацию ключей шифрования, который, используя случайное число, передаваемое на мобильный терминал в момент соединения с сетью, и ключ Ki генерит 64-битный ключ шифрования трафика. Так как индивидуальный ключ Ki имеется не только у абонента, но и хранится в реестрах HLR и VLR, то и абонент и оборудование сети создают одинаковый ключ шифрования, который и используется для защиты передаваемых данных.

Алгоритм A3, отвечающий за аутентификацию абонента, похож на алгоритм A8 и также использует случайное число, получаемое в момент подключения к сети и индивидуальный ключ абонента.

Для доступа к функциям SIM-карты необходимо использовать специальный персональный код (другими словами, пароль) PIN (Personal Identiёcation Number), после 3-х неправильных попыток ввода которого, SIM-карта блокируется.

Безопасность самого телефона, как уже было сказано выше, обеспечивается двумя механизмами:

алгоритмом шифрования A5, который обеспечивает защиту данных, циркулируемых между мобильной станцией и узлом SGSN.

Уникальным 14-тиразрядным международным идентификатором аппаратуры мобильной связи (International Mobile Equipment Identity, IMEI), который однозначно идентифицирует телефон. Узнать этот номер очень просто - достаточно набрать на телефоне комбинацию \*#06#. Если высвеченное число не совпадает с тем, что указано на задней крышке телефона, то вероятнее всего вы пользуетесь взломанным аппаратом. Именно эти номера хранятся в реестре EIR. Данный реестр ведет три типа списков IMEI:

"белый" список, содержащий идентификаторы всех разрешенных аппаратов.

"серый" список, содержащий идентификаторы всех незапрещенных аппаратов, но используемых для различных целей, например, тестирования и т.п.

"черный" список, содержащий идентификаторы всех запрещенных аппаратов. Как заявил в одном из интервью вице-президент МТС (http://www.mts.ru/press/speech9.html) Михаил Сусов "Сейчас между операторами (в России - А.Л.) проводятся переговоры о создании единого "черного списка" краденых телефонов".

Надо понимать, что идентификаторы IMEI и IMSI - независимы между собой. Более того - они решают различные задачи: IMEI идентифицирует мобильный терминал, а IMSI - абонента.

Безопасность соединения мобильной станции с узлом SGSN

В процессе подключения мобильной станции, описываемом далее, между ней и узлом SGSN происходит выбор версии используемого в дальнейшем алгоритма шифрования GPRS-A5. В 3-м квартале 2002 года началось внедрение третьей версии этого алгоритма (A5/3), которая может использоваться не только в GSM-, но и в GPRS-, HSCSD- и EDGE-сетях. Данный алгоритм разработан на базе алгоритма "Казуми" (Kasumi), в свою очередь разработанного на базе алгоритма MISTY компании Мицубиси. Как утверждается в пресс-релизе Ассоциации GSM (http://www.gsmworld.com/news/press\_2002/press\_15.shtml), A5/3 обеспечивает на сегодняшний день практически 100-процентную защиту передаваемых данных. Однако не стоить безоглядно верить этому утверждению. Аналогичные заявления делались и для предыдущих версий алгоритма A5, история которого начинается с 1987 года, однако они были успешно взломаны.

В сетях GPRS используются алгоритмы семейства A5 - GEA1 и GEA2, а после разработки A5/3 - начинается внедрение созданного на его базе алгоритма GEA3.

Безопасность данных в процессе их передачи по сети GPRS

Все данные между узлами поддержки (SGSN и GGSN) передаются с помощью специального протокола GTP (GPRS Tunneling Protocol), который инкапсулирует в себя любые пользовательские протоколы, например, HTTP, Telnet, FTP и т.д. По умолчанию GTP-трафик не шифруется. Кроме того, опорная сеть строится на базе частных IP-адресов, описанных в RFC 1918 (http://www.ietf.org/rfc/rfc1918.txt), что обеспечивает невозможность прямого доступа к сетевому оборудованию из внешних сетей.

Безопасность в процессе взаимодействия с различными операторами GPRS-услуг

Безопасность возлагается на устройства, называемые пограничными шлюзами (border gateway, BG), которые очень похожи на обычные межсетевые экраны, защищающие корпоративные сети от посягательств злоумышленников. В частности, этот шлюз защищает оператора от атак, связанных с подменой адреса (IP Spooёng).

Настройка такого шлюза включает в себя создание правил, разрешающих входящий/исходящий пользовательский трафик, данные биллинговой системы, аутентификацию роуминговых абонентов и т.п. Дополнительно на пограничный шлюз может быть установлено программное обеспечение, организующее VPN между различными GPRS-операторами.

Помимо встроенных в пограничный шлюз защитных механизмов, существует возможность использования продуктов третьих фирм. Первым таким решением стал межсетевой экран Firewall-1 GX компании CheckPoint Software (http://www.checkpoint.com/products/solutions/ёrewall-1gx.html), который, будучи установлен на пограничном шлюзе или узле GGSN повышает защищенность сети GPRS-оператора от возможных несанкционированных действий.

Безопасность в процессе взаимодействия с Internet

Основные механизмы безопасности реализованы на узле GGSN, в состав которого входит межсетевой экран, который определяет тип входящего и исходящего GPRS-трафика. Задача межсетевого экрана, входящего в состав GGSN, защитить мобильную станцию от атак внешних (из Internet) хакеров. Защита от атак с других мобильных станций возлагается на узел SGSN. Для предотвращения доступа к сетевому оборудованию опорной сети от внешних злоумышленников используется трансляция адресов (network address translation). Все остальные механизмы защиты могут быть взяты из классической практики обеспечения информационной безопасности Internet-сетей и устройств, например, аутентификация при помощи серверов RADIUS или защита трафика с помощью IPSec.

Процедура подключения мобильной станции

Упрощенно процесс подключения абонента, желающего воспользоваться услугами GPRS, выглядит следующим образом:

Мобильная станция посылает запрос (Attach Request) на получение доступа к сети, который содержит ряд параметров, в т.ч. и IMSI.

Узел SGSN, получив такой запрос, проверяет наличие аутентифицирующей данного абонента информации в своей базе. Если такая информация отсутствует, то SGSN посылает запрос в реестр HLR, который возвращаетт.н. аутентификационный триплет, содержащий:

Случайное число, используемое в алгоритмах A3 и A8 для выработки ключа шифрования и аутентификации абонента.

32-хразрядный ключ аутентификации абонента, который вырабатывается на основе индивидуального ключа, хранящегося как на мобильной станции, так и в реестре HLR.

Ключ шифрования данных, получаемый также на базе индивидуального ключа абонента.

Полученное случайное число передается на мобильную станцию, которая на его основе вырабатывает ключ шифрования и ключ аутентификации. Т.к. индивидуальные ключи, хранящиеся в реестре HLR и на мобильной станции совпадают, то и ключи шифрования и аутентификации также должны совпадать, что и является фактом правомочности запроса данным абонентом оплаченных GPRS-услуг.

После идентификации абонента осуществляется идентификация оборудования, которое посылает на SGSN идентификатор IMEI. Узел SGSN в свою очередь проводит проверку данного оборудования по реестру EIR.

После аутентификации абонента и оборудования происходит процедура определения местоположения абонента (с использованием реестров HLR и VLR), после чего происходит завершение процедуры подключения мобильной станции к сети GPRS. В том случае, если мобильная станция не смогла пройти аутентификацию, то SGSN посылает на нее сообщение Attach Reject.

**Заключение**

В заключение хочу добавить, что, при создании технологии GPRS (как и при создании многих современных сетевых технологий) вопросам безопасности внимания уделялось недостаточно. Многие аспекты не описаны и отданы на откуп операторам, которые далеко не всегда уделяет безопасности первостепенное внимание, что приводит к печальным последствиям. Специалистами найдено уже немало недостатков технологии GPRS, но это уже тема другой статьи