Московский физико-технический институт (Государственный Университет)
Кафедра Радиотехники

Эссе по курсу «Защита информации»

на тему «Безопасность технологии GPRS»

студента 116 группы Фадина Д.Ю.

Москва, 2005г.

Введение

GPRS (General Packet Radio Service) – услуга пакетной передачи данных по радиоканалу, которая была разработана главным образом для возможности работать в сети Интернет при помощи обычного сотового телефона. Разработчики технологии GPRS постарались принцип ее работы как можно сильнее приблизить к технологии GSM, чтобы ведущие компании, предоставляющие услуги сотовой связи стандарта GSM, смогли быстро и с минимальными затратами внедрить технологию GPRS. Однако, GPRS имеет также существенные отличия от GSM, главное из которых состоит в том, что ресурсы сети (каналы) задействованы только во время передачи данных, благодаря пакетному способу передачи данных. Это позволило, во-первых, увеличить эффективность используемых ресурсов, а вместе с ней и скорость передачи данных, так и, во-вторых, брать с пользователей плату только за объем передаваемой информации, а не за время нахождения в сети в режиме «on-line», как это сейчас происходит в сетях GSM.

Архитектура сети GPRS

Перед тем как рассматривать вопрос о безопасности GPRS и о ее слабых местах, надо разобраться в архитектуре GPRS. Общий вид системы GPRS представлен на рисунке:

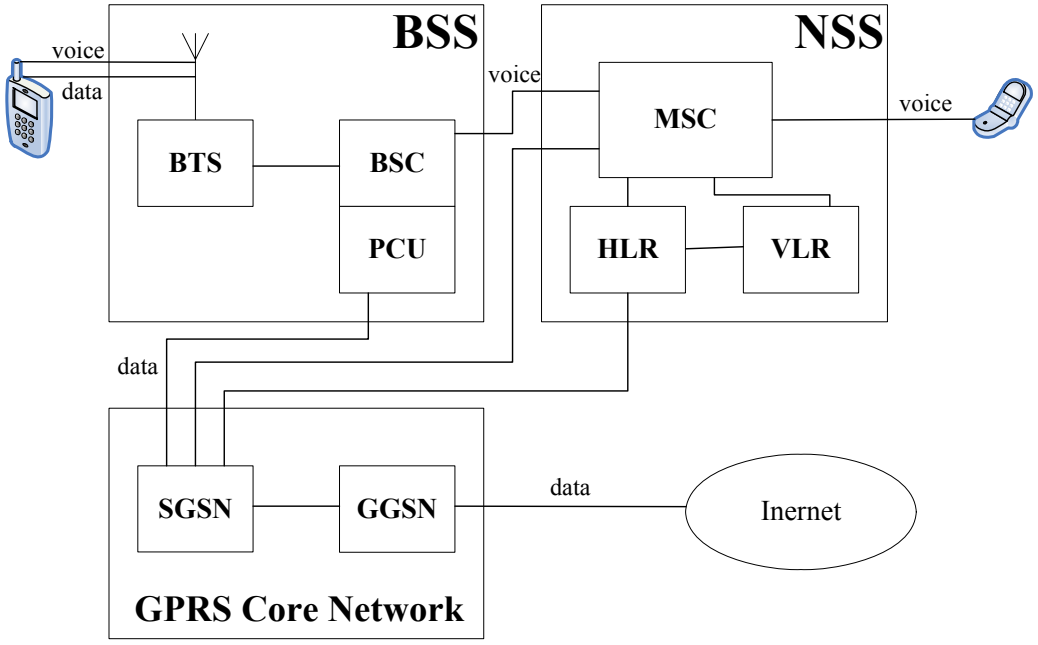

Рис. 1. Архитектура GPRS-сети.

В состав GPRS-сети входят 4 основных компонента:

- **мобильная станция** (Mobile Station, MS),
- **базовая станция** (Base Station System, BSS),
- **узел обслуживания абонентов** (Serving GPRS Support Node, SGSN),
- **узел маршрутизации GPRS** (Gateway GPRS Support Node, GGSN).

Так же в состав GPRS-сети входят 3 типа реестров:

- **реестр собственных абонентов сети** (Home Location Register, HLR),
- **реестр перемещений** (Visitor Location Register, VLR),

- **реестр идентификационных данных оборудования** (Equipment Identity Register, EIR).

Мобильная станция

Под мобильной станцией обычно понимается оборудование, которое позволяет абоненту работать в сети Инетрнет. Функционально, его можно разделить на две части:

- Терминальное оборудование (terminal equipment, TE)
- Мобильный терминал (mobile terminal, MB)

Терминальное оборудование позволяет пользоваться Интернетом (просматривать сайты, читать почту и т д.), а мобильный терминал осуществляет связь мобильной станции с базовой станцией GPRS-сети и передачу данных.

В качестве TE часто используются переносные, карманные, а иногда и стационарные компьютеры. В качестве MT обычно используются сотовые телефоны, поддерживающие GPRS, но в последнее время все большую популярность приобретают так называемые GPRS-модемы, которые позволяют пользоваться Интернетом при помощи услуги GPRS владельцам ноутбуков и даже обычных персональных (стационарных) компьютеров.

С точки зрения классификации режимов работы, все мобильные станции можно разделить на 3 класса. Класс, к которому принадлежит данная MS, определяется возможностями оборудования и возможностями сети:

- **Класс A.** При помощи MS класса A пользователь может одновременно передавать и данные, при помощи технологии GPRS, и голос, при помощи, например, технологии GSM.
- **Класс B**. При помощи MS класса B пользователь может передавать и данные, и голос, но в разные моменты времени. Типичный пример мобильной станции данного класса – сотовый телефон, поддерживающий технологию GPRS.
- **Класс C.** При помощи MS класса C пользователь может передавать только пакеты данных, то есть работать только в сети GPRS. Примером такого оборудования могут служить карты PCMCIA, CF и USB адаптеры.

Базовая станция

Главные функции BS это: принять радиосигнал от MS (или наоборот, отправить его на MS), распознать этот сигнал (узнать, что это за сигнал: голос или пакетные данные, так как сети GPRS и GSM используют одинаковые частоты, что исключает возможность распознавания сигнала по частоте) и в зависимости от того, что передается, передать трафик на:

- MSC (mobile switching center) – центр коммутации, являющийся стандартным элементом GSM-сети
- SGSN

Получается, что базовая станция является общим элементом GPRS и GSM сетей, что, несомненно, «радует» операторов сотовой связи.

Базовая станция состоит из **приемно-передающей базовой станции** (BTS, Base Transereceiver Station), которая осуществляет прием и передачу информации между антенной и BSC; из **контроллера базовой станции** (BSC, Base Station Controller), основная функция которого – управление распределением радиоканалов и разделении

информации на данные и голосовую; **устройства контроля пакетной передачи** (PCU, Packet Control Unit), которое стыкуется с контроллером базовых станций BSC и отвечает за направление трафика данных непосредственно от BSC к SGSN.

Узел обслуживание абонентов GPRS

SGSN – один из важнейших элементов GPRS-сети. По сути, SGSN – аналог MSC в сети GSM. Только в отличие от MSC, SGSN работает с пакетными данными, а не с голосовыми данными.

SGSN при помощи баз данных, хранящихся в реестрах HLR, VLR и EIR, обеспечивает подключение нового абонента к сети; защиту GPRS от таких атак, как несанкционированное подключение к сети, подключение к сети с украденного или взломанного оборудования; шифрует данные (IP-пакеты) при помощи алгоритмов GEA1, GEA2 и GEA3. Подробнее механизмы обеспечения безопасности, которые осуществляются при помощи SGSN будут описаны ниже.

Узел маршрутизации GPRS

GGSN также как и SGSN является важнейшим элементом GPRS-сети, как с точки зрения функционирования сети, так и с точки зрения обеспечения безопасности этого функционирования. С точки зрения обеспечения функционирования сети GPRS GGSN выполняет такие важные функции, как прием и передача данных из внешних сетей (Интернет, GPRS-сеть другого оператора, если абонент использует услугу роуминга, и т. д.), выдача IP-адресов абонентам и тарификации их услуг. С точки зрения обеспечения безопасности сети GPRS, GGSN защищает сеть от атак из вне (Интернет, GPRS-сеть другого оператора и т. д.) Подробнее об обеспечении защиты от такого рода атак будет написано ниже.

Реестры GPRS-сети

Реестры в GPRS-сетях – это «хранилища», которые содержат базы данных с информацией об абонентах сети (в том числе и об услугах, которые предоставляются абоненту) или об используемом оборудовании. В GPRS можно выделить три основных реестра: HLR, VLR и EIR.

HLR – реестр собственных абонентов сети. Уже по названию данного реестра понятно, что он хранит в себе базу данных, в которой содержатся все абоненты сети GPRS, оплатившие услуги оператора именно этой сети (а не какой-нибудь другой). Помимо информации о стандартных услугах, которые предоставляет технология GPRS, HLR содержит также информацию о том, какие абоненты какие дополнительные услуги подключили и оплатили. Также HLR содержит параметры аутентификации каждого абонента (аутентификационный триплет, о котором будет рассказано во время описания механизма аутентификации абонента). В сети GPRS HLR обменивается данными только с SGSN.

VLR – реестр перемещений. VLR содержит ту же самую информацию об абонентах, что и HLR, но не всех, а только тех абонентов, которые в данный момент находятся в географической зоне, обслуживаемой этим VLR. Информация о новом абоненте заносится в VLR сразу же, как только абонент появляется в зоне действия данного VLR. Обмен данных происходит между HLR и VLR.

EIR – реестр идентификационных данных оборудования, который хранит в себе информацию о терминальном оборудовании, чтобы блокировать вызовы от украденных, «серых» или неавторизованных устройств. Обмен данных происходит между EIR и SGSN.

Ниже, во время описания механизма аутентификации абонентов в сети GPRS, будет рассказано о том, какая именно информация содержится в этих реестрах, и на каких этапах и как она используется.

Вот в принципе и все, что необходимо знать об архитектуре GPRS-сети, чтобы разобраться в механизмах обеспечения ее безопасности.

Механизмы безопасности GPRS-сети на различных участках

В сети GPRS можно выделить следующие фрагменты, на безопасность которых нужно обратить внимание:

- Безопасность MS
- Безопасность передачи данных между MS и SGSN
- Безопасность передачи данных между SGSN и GGSN
- Безопасность передачи данных между различными операторами GPRS-услуг
- Безопасность передачи данных в сети открытого доступа

Безопасность мобильной станции

В области обеспечения безопасности мобильной станции GPRS практически ничем не отличается от GSM. В качестве мобильной станции, рассмотрим обычный сотовый телефон. С точки зрения безопасности телефон можно разделить на две составляющие:

- SIM-карта
- Сам телефон (трубка)

SIM-карта (Subscriber Identity Module) – это в некотором смысле паспорт абонента, содержащий в себе информацию об абоненте, при помощи которой абонент пользуется всеми подключенными и оплаченными услугами. Если SIM-карту можно физически извлечь из телефона, не применяя грубой силы, а это возможно сделать на большинстве GSM-телефонах, то ее можно использовать на любом другом GSM-телефоне. При этом также можно пользоваться всеми подключенными и оплаченными услугами.

Для обеспечения защиты от несанкционированного доступа в сеть, в SIM-карте содержатся:

- IMSI (International Mobile Subscriber Identity), идентификатор абонента, который в свою очередь включает в себя:
  - Трехразрядный код страны (РФ – 250)
  - Двухразрядный код сети
  - Десятиразрядный код абонента MSIN (Mobile Subscriber Identity Number)
- Собственный индивидуальный ключ аутентификации Ki, копия которого хранится в HLR и VLR. Длина Ki – 128 бит
- Алгоритм аутентификации A3
- Алгоритм генерации ключей шифрования A8

- Четырехразрядный PIN-код (Personal Identification Number) для защиты SIM-карты в случае кражи. После трех неправильных вводов PIN-кода SIM-карта блокируется.

Безопасность телефона, как терминального оборудования, обеспечивается уникальным 14-разрядным международным идентификатором аппаратуры мобильной связи (IMEI, International Mobile Equipment Identity). IMEI однозначно идентифицирует телефон и при помощи регистра EIR на стадии аутентификации абонента пускает или не пускает его в сеть (о том, как используется IMEI написано в механизме аутентификации абонента).

Если на телефоне набрать комбинацию *#06#, то IMEI высветится на экране. Если высвеченное число не совпадает с тем, что указано на задней крышке телефона (под аккумулятором), то телефон взломан. IMEI хранится в реестре EIR, о котором упоминалось выше. EIR содержит три списка IMEI:

- «белый», который содержит IMEI всех разрешенных аппаратов;
- «серый», который содержит IMEI всех незапрещенных аппаратов;
- «черный», который содержит IMEI всех запрещенных аппаратов (в том числе и украденных).

Таким образом, получаем, что IMEI идентифицирует оборудование, а IMSI – абонента.

Теперь пришло время рассмотреть, как происходит процесс аутентификации абонента и оборудования при помощи идентификаторов, ключей и алгоритмов, которые были описаны выше.

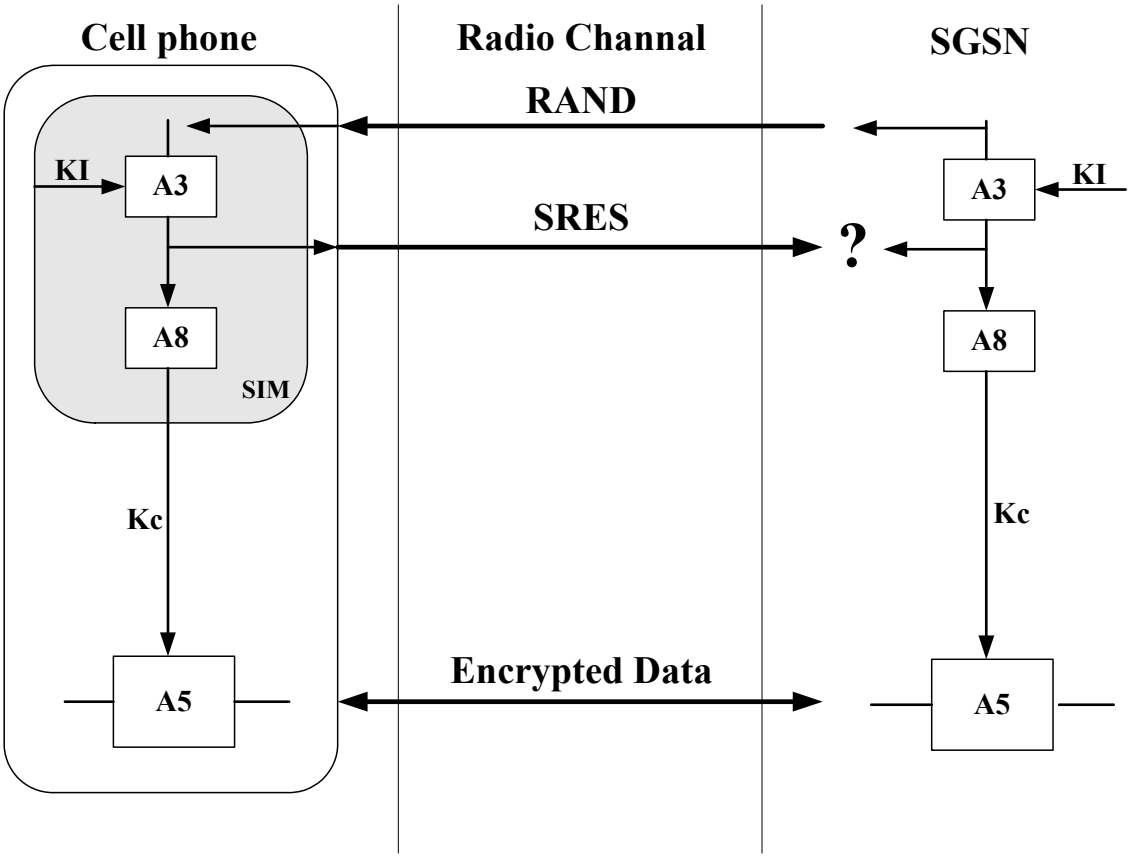

Рис. 2. Схема аутентификации абонента.

Аутентификация пользователя осуществляется следующим образом:

1. MS посылает по радиоканалу запрос (Attach Request) узлу SGSN на получение доступа к услугам сети. В этом запросе содержится IMSI, при помощи которого SGSN идентифицирует абонента.
2. Если в базе данных SGSN нет аутентифицирующей данного абонента информации, то SGSN посылает запрос в HLR, который возвращает SGSN так называемый аутентификационный триплет, содержащий:
    - Случайное число RAND (128 бит)
    - Ключ Ki (128 бит)
    - Ключ Kc (64 бита)
3. SGSN посылает RAND на MS по тому же самому радиоканалу. SIM-карта производит вычисления по алгоритму A3, на вход которого подается RAND, а в качестве ключа используется Ki, содержащийся в самой карте. В результате получается последовательность SRES (Signed RESponse – подписанный ответ), отправляющаяся обратно. SGSN так же вычисляет SRES по алгоритму A3, используя ключ Ki, который он получил от HLR в составе триплета. Если результаты вычисления SRES на SIM-карте и в SGSN совпадают, то аутентификация абонента завершается успешно.
4. После того, как абонент аутентифицировался, происходит аутентификация оборудования следующим образом: MS посылает на SGSN идентификатор IMEI. SGSN проводит проверку данного оборудования по реестру EIR.
5. Если аутентификации абонента и оборудования прошли успешно, то происходит процесс определения местоположения абонента с использованием реестров HLR и VLR, после чего происходит завершение процедуры подключения MS к сети GPRS

Если MS на каком-то этапе аутентификации не проходит ее, то SGSN посылает на нее сообщение Attach Reject о том, что аутентификация не пройдена.

Получается, что обеспечение безопасности мобильной MS от несанкционированного подключения осуществляется благодаря идентификаторам IMEI и IMSI, алгоритмом аутентификации A3 и ключом Ki, используемом алгоритмом A3. В принципе, аутентификация абонента и оборудования в сети GPRS имеет высокую степень защиты, и чтобы злоумышленникам проникнуть в сеть таким способом, им придется сильно попотеть. Однако, данный алгоритм аутентифицирует только абонента, но не аутентифицирует практически никак MS, благодаря чему она может быть успешно подменена (если, конечно, злоумышленники знают ключ Ki или Kc). В результате чего, информация, идущая от абонента, может перехватываться, причем абонент даже не будет знать об этом, а абоненту может даваться ложная информация.

Безопасность соединения между мобильной станцией и узлом SGSN

Безопасность передачи данных между MS и SGSN обеспечивается алгоритмом шифрования A5, который использует ключ Kc, сгенерированный алгоритмом A8. Длина Kc – 64 бита.

Существует несколько видов алгоритма шифрования передаваемых данных GPRS-A5: GEA1, GEA2 и GEA3. Выбор конкретного алгоритма происходит во время подключения и аутентификации MS. В настоящее время считается, что алгоритм GEA3 дает практически 100 процентную защиту, правда аналогичные заявления делались и относительно алгоритмов A5/1 и A5/2 (A5/1 и A5/2 – алгоритмы шифрования в сетях

GSM, аналогами которых являются алгоритмы GEA1 и GEA2 в сетях GPRS), которые на данный момент успешно взломаны.

В процессе передачи данных между MS и SGSN, кроме того, что данные передаются по радиоканалу и могут быть легко перехвачены злоумышленниками при помощи специальных технических устройств и дешифрованы, существует ещё как минимум две серьезные проблемы:

1) Большинство операторов GPRS-услуг используют устаревшие алгоритмы шифрования данных, которые имеют недостаточную длину ключа шифрования, в результате чего могут быть взломаны, несмотря на дороговизну оборудования для взлома.
2) Из-за увеличения в последнее время террористической угрозы, спецслужбы многих стран (например ФСБ, ФАПСИ, ФБР, ЦРУ и т. д.) получили право заставлять операторов GPRS-услуг отключать шифрование, чтобы перехватывать данные у террористов. В результате этого, злоумышленники могут воспользоваться этим в своих целях и могут пострадать обычные абоненты GPRS-сети.

Безопасность соединения между узлами SGSN и GGSN.

Для обеспечения безопасности передачи пакетов между узлами обслуживания и маршрутизации, было решено использовать протокол GTP (GPRS Tunneling Protocol), что позволило обессилить обычные хакерские инструменты. Обычно GTP-трафик не шифруется, но в принципе оператор GPRS-услуг сам решает шифровать трафик или нет. GTP-протокол инкапсулирует в себя любые пользовательские протоколы, например, HTTP, Telnet, FTP и т. д.

Чтобы уменьшить возможность проникновения злоумышленников из вне (например, из Интернета), опорная сеть построена на базе частных (локальных) IP-адресов. Другие механизмы обеспечения безопасности сети GPRS от атак из вне описаны ниже.

Безопасность данных при их передаче между различными операторами GPRS-услуг

В процессе взаимодействия различных операторов GPRS-услуг безопасность передачи данных обеспечивается при помощи пограничных шлюзов (Border Gateway, BG). По сути дела BG – это обычный межсетевой экран (Firewall), который защищает обычные корпоративные сети от атак из вне. Межсетевой экран представляет собой «ограждение» вокруг сети.

Основная опасность, которая содержится в данном методе, заключается в том, что после установки, BG нужно настроить (создать правила прохода информации через «ограждение»). Пограничные шлюзы настраивают администраторы «вручную» и в этих настройках неизбежны «слабые места». Именно этот факт (наличие слабых мест или ошибки в настройках шлюзов) и используется многими злоумышленниками.

Для повышения защищенности канала, соединяющего GPRS-сети различных операторов, на пограничный шлюз можно установить программное обеспечение, организующее VPN (Virtual Private Network) между этими GPRS-операторами.

Безопасность данных при их передаче в сети открытого доступа

При взаимодействии с сетью Интернет защиту GPRS-сети обеспечивает узел GGSN. Защита обеспечивается при помощи межсетевого экрана, настроенного на защиту

стандартных атак хакеров из Интернета. Чтобы уменьшить вероятность атак из вне помимо того, что опорная сеть строится на базе частных IP-адресов, наряду с этим используется трансляция адресов (network address translation).

Подытожим все вышесказанное в виде таблицы:

Возможные атаки на сеть GPRS	**Механизм борьбы**	**Слабые места механизма**
Несанкционированное подключение мобильной станции	Аутентификация, в которой используются идентификаторы IMEI, IMSI, аутентификационный ключ Ki. PIN-код для защиты телефона в случае потери или кражи.	PIN-код нужно вводить только при включении телефона, в остальных случаях PIN-код вводить не нужно; SIM-карту можно просканировать украдкой от хозяина и сделать ее точную копию
Подмена базовой станции	Отсутствует, так как оборудование для подмены базовой станции стоит достаточно дорого, в результате чего этот метод подслушивания информации оказывается неэффективным	
Атака на соединение между MS и SGSN	Алгоритм шифрования A5, ключ к которому генерируется во время подключения	Алгоритм A5 известен, ключ можно подобрать, а радиосигнал перехватить
Атака на соединение между SGSN и GGSN	Протокол передачи данных GTP, опорная сеть на базе частных IP-адресов	Осуществления атаки типа GTP Signaling Flood или других атак, которые занимают ресурсы сети и ухудшают качество функционирования сети; ошибки настроек администраторов
Атака на сеть из GPRS-сети другого оператора	Пограничные шлюзы (Border Gateway); виртуальная частная сеть (VPN) между различными операторами GPRS-сети	Шлюзы настраиваются вручную администраторами, поэтому не исключены ошибки или слабые места в настройках конфигурации
Атака на сеть из Интернета	Межсетевой экран, опорная сеть на базе частных IP-адресов, трансляция адресов	Межсетевые экраны настраиваются вручную администраторами, поэтому не исключены ошибки или слабые места в настройках конфигурации

Использованная литература.

1. Марат Давлетханов. «Безопасность GPRS.» http://infobez.ru/article.asp?ob_no=1740
2. Что такое GPRS? (Автор неизвестен.) http://pro-wap.nm.ru/index.files/Page6398.htm