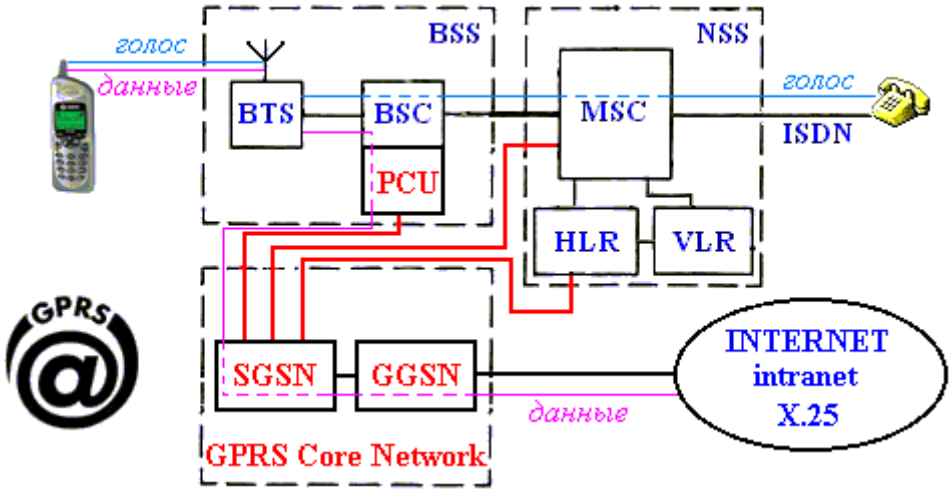
Фатхуллин Ринат Маратович
группа 013

БЕЗОПАСНОСТЬ ТЕХНОЛОГИИ GPRS.

GPRS (General Packet Radio Service – услуга пакетной передачи данных по радиоканалу) - перспективная технология, стандартизация которой началась в 1993 году в ETSI (European Telecommunication Standards Institute). Она позволяет работать в сети Internet, используя обычный мобильный телефон. С помощью GPRS, пользователю доступны электронная почта и обычно Web-серверы (а не со специальными WAP-версиями) и многое другое. GPRS была разработана для высокоскоростной передачи данных посредством существующих GSM сетей. Кроме того, данная система предполагает иную систему оплаты услуги передачи данных – расчеты производятся пропорционально объему трафика – количеству информации, переданной и полученной абонентом, а не времени, проведенному в сети.

GPRS появилась как надстройка над существующими сетями GSM, ее разработчики приложили максимум усилий, чтобы ее установка оказалась как можно менее обременительной и разорительной для операторов. Ниже рассматривается, какие новые блоки и связи появились в общей архитектуре системы сотовой связи стандарта GSM с внедрением GPRS, а потом обсуждается, какие проблемы безопасности при этом возникают и какие существуют методы борьбы с ними.

Архитектура GPRS расширяет стандартные компоненты GSM новыми или обновленными элементами. Таких элементов всего 4, причем лишь 2 из них не были известны в GSM. Общий вид системы GPRS представлен на рисунке 1.



Ядро системы GPRS (GPRS Core Network) состоит из двух основных блоков - SGSN (Serving GPRS Support Node - узел поддержки GPRS/узел обслуживания абонентов) и GGPRS (Gateway GPRS Support Node - шлюзовой узел GPRS).

SGSN является, по сути, мозгом рассматриваемой системы. Он контролирует доставку пакетов данных пользователям, взаимодействует с реестром собственных абонентов сети HLR, проверяя, разрешены ли запрашиваемые пользователями услуги, ведет мониторинг находящихся online пользователей, организует регистрацию абонентов вновь "проявившихся" в зоне действия сети. Как правило, такой узел построен на базе ОС Unix и имеет свой IP-адрес. Отметим, что этот факт также может быть использован злоумышленниками для поиска уязвимости GPRS.

С точки зрения безопасности, на SGSN возложены функции:
1. Проверки разрешений абонентов на пользование запрашиваемых услуг (аутентификация).
2. Мониторинг активных абонентов.
3. Регистрация новых абонентов.
4. 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.

Рассмотрим эти функции более подробно.

1. Аутентификация GPRS полностью совпадает с аналогичным механизмом в GSM. Интересующиеся могут обратиться к [1], чтобы получить исчерпывающую информацию об этом.

2. Для быстрой маршрутизации информации к мобильному абоненту GPRS-система нуждается в данных о его месторасположении относительно сети, причем с большей точностью, нежели в случае передачи голосового трафика. Однако это было бы неразумным с точки зрения объема передаваемого трафика и необходимой мощностью батарей передавать системе информацию о местоположении абонента каждый раз, когда это необходимо. Чтобы найти разумный компромисс между объемом сигнального трафика в сети GPRS и необходимостью знать с высокой точностью местонахождение абонента принято деление терминалов на три класса:

- IDLE (неработающий). Телефон отключен или находится вне зоны действия сети. Очевидно, что система не отслеживает перемещение подобных абонентов.
- STANDBY (режим ожидания). Аппарат зарегистрирован (прикреплен) в GPRS-системе, но уже долгое время (определяемое специальным таймером) не работает с передачей данных. Местоположение STANDBY-абонентов известно с точностью до RA (Routing Area - область маршрутизации). RA мельче, чем LA (каждая LA разбивается на несколько RA, но, тем не менее, RA крупнее, чем сота, и состоит из нескольких элементарных ячеек).
- READY (готовность). Абонентский терминал зарегистрирован в системе и находится в активной работе. Координаты телефонов, находящихся в режиме READY, известны системе (а, точнее, SGSN) с точностью до соты.

Согласно этой идеологии, терминалы, находящиеся в STANDBY-режиме, при переходе из одного RA в другой посылают SGSN специальный сигнал о смене области маршрутизации (routing area update request). Если новая и старая RA контролируется одним SGSN, то смена RA приводит лишь к корректировке записи в SGSN. Если же абонент переходит в зону действия нового SGSN, то новый SGSN запрашивает у старого информацию о пользователе, а MSC, VLR, HLR и вовлеченные в работу GGSN ставятся в известность о смене SGSN. Когда телефон, работающий с GPRS-системой, перемещается в другую LA, то SGSN отправляет соответствующему VLR сообщение о необходимости смены записи о местонахождении абонента.

3. 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 возвращает т.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.
4. В процессе подключения мобильной станции 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

Предназначение GGSN можно понять из его названия - грубо говоря, это шлюз между сотовой сетью (вернее, ее частью для передачи данных GPRS) и внешними информационными магистралями (Internet, корпоративными интранет-сетями, другими GPRS системами и так далее). Основной задачей GGSN, таким образом, является роутинг (маршрутизация) данных, идущих от и к абоненту через SGSN. Вторичными функциями GGSN является адресация данных, динамическая выдача IP-адресов, а также отслеживание информации о внешних сетях и собственных абонентах (в том числе тарификация услуг).
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.

Еще одной составной частью системы GPRS является PCU (Packet Control Unit - устройство контроля пакетной передачи). PCU стыкуется с контроллером базовых станций BSC и отвечает за направление трафика данных непосредственно от BSC к SGSN.

Еще два элемента, добавленные в GPRS – это мобильная и базовая станции.
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.
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.
Вопросы безопасности мобильной станции широко освещены в различных изданиях. Интересными могут показаться [2,3]. Отметим лишь основные положения. Безопасность мобильной станции складывается из 2 положений:
- SIM карта
- сам телефон.
Каждый абонент в сети GPRS имеет уникальный международный идентификатор мобильного телефона (IMSI, International Mobile Subscriber Identity), хранимый с SIM-карте. Кроме того, карта хранит индивидуальный ключ аутентификации абонента длиной 128 бит Ki, алгоритм генерации ключей шифрования A8, алгоритм аутентификации A3 и разумеется PIN-код для доступа к функциям самой карты. 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. Именно эти номера хранятся в реестре EIR.

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 Spoofing).
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/firewall-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.

На текущее время известны следующие уязвимости технологии GPRS:

1. Отказ в обслуживании обнаружен в Nokia Gateway GPRS Support Node (GGSN)[4]. Уязвимость состоит в том, что удаленный пользователь может нарушить работу ядра. Сообщается, что GGSN содержит недостаток в выполнении TCP стека. Удаленный пользователь может послать специально сформированный пакет с TCP опцией 0xFF, через мобильный телефон, чтобы аварийно завершить работу системы, и остановить передачу данных в GPRS сети. GGSN автоматически перезагрузится после аварии системы. Согласно сообщению, все операторы сотовой связи были предупреждены и сделали соответствующие обновления. Уязвимость обнаружена в Nokia Gateway GPRS Support Node (GGSN).
2. Одной из наиболее критичных с точки зрения безопасности с сети GPRS является точка доступа роуминговых абонентов, иными словами - шлюз в сети партнеров. Так как в сети GRPS используется IP-протокол, практически любой из абонентов сетей роуминговых партнеров может посылать пакеты в нашу сеть. Поэтому вход в магистральную сеть оператора должен быть надежно защищен межсетевым экраном (МСЭ), учитывающим специфику протокола GTP. В модели доверительных отношений протокола GTP существует множество потенциальных угроз безопасности. К таким угрозам относятся атаки переполнения сети (отказ в обслуживании), подмена IP-адресов (спуфинг), вмешательство в чужую сессию (туннель) и некорректные попытки установки соединений.
3. Проблемы безопасности в GTP.
Принцип организации GTP-туннелей отличается от других IP-протоколов. Эти различия скрываются на нескольких уровнях работы: Одна IP-сессия может содержать в себе несколько туннелей; один туннель может быть "размазан" по нескольким IP-сессиям; и туннели могут "перескакивать" между IP-сессиями в процессе перенаправления или передачи от одной базовой станции к другой. Такой принцип работы делает практически бесполезным применение классических IP-Firewall для фильтрации GTP-трафика.
4. SGSN Handover.

Коммутаторы SGSN (коммутатор преобразования пакетов GSM в пакеты IP) могут передавать существующие GTP-туннели на другие базовые станции с помощью процедур

"Routing Area Update". Эта функция GPRS подвергает шлюзы GGSN (шлюз связи сети GPRS с сетями TCP/IP) серьезным опасностям, так как передача туннеля другому коммутатору проводится безо всякой аутентификации.
5. Переполнение сети. Аналогично атакам типа SYN-flooding в TCP, в сетях GPRS могут быть осуществлены атаки типа GTP Signaling Flood, которые занимают значительный объем полезной полосы пропускания каналов, процессорные и другие ресурсы шлюза GGSN, что приводит к резкому ухудшению качества обслуживания пользователей GRPS-сети.
6. Ошибки в конфигурации сети. Ошибки администратора могут привести к появлению серьезных уязвимостей в GPRS-системе оператора. Наиболее часто встречающиеся ошибки - неправильная настройка маршрутизации, ошибки APN, сбои DNS серверов, а также различные ошибки базы данных. Это происходит из-за того, что IP - это открытый протокол и используется во многих магистральных и локальных сетях. Большинство операторов использует одни и те же каналы для различных типов трафика, и это особенно актуально при использовании роуминга. Стандартная IP-отчетность не дает полной картины. Она не содержит в себе информацию о параметрах GTP, которые так важны для администраторов сетей GPRS и 3G, чтобы они могли отслеживать работу пользователей и фиксировать все нарушения политики безопасности. К таким GTP-специфичным параметрам относятся IMSI, MS-ISDN, APN и другие информационные поля протоколов 3G.

Основные функциональные особенности оптимального решения (специализированного МСЭ) для обеспечения безопасности внутреннего и роумингового трафика с учетом специфики GTP:
Полное соответствие стандартам 3GPP GPRS;
Проверка целостности пакетов в протоколе GTP, а также внутренней морфологии;
Подробный анализ и управление туннелями;
Управление роуминговыми ограничениями, политиками перенаправления и переключения соединений на базовых станциях;
Анализ информационных элементов GTP;
Генерация отчетов и предупреждений с указанием всей GTP-специфичной информации;
Все это не допускает перегрузок сети вредоносными пакетами, позволяет оператору создавать политику безопасности, учитывающую специфику GTP. Для защиты критичных элементов GPRS-инфраструктуры целесообразно устанавливать специализированные межсетевые экраны на Gp-интерфейсе (между домашней PLMN и сетью GRX) и Gn-интерфейсе (между узлами SGSN и GGSN в домашней PLMN). В сочетании со стандартным межсетевым экраном на интерфейсе Gi такое решение обеспечивает наивысший уровень защиты.

HLR (Home Location Register) - регистр местоположения собственных абонентов.
VLR (Visitor Location Register) - регистр местоположения обслуживаемых абонентов.
APN (access point name) – имя точки доступа в Интернет.

Использованные материалы

1. “GSM:безопасность вашей информации”; [автор неизвестен]. http://www.bnti.ru/scripts/showart.asp?lvl=03.07.&tbl=&aid=249
2. “GSM: мифы и реальность”; [автор неизвестен]. http://gsmzone.com.ua/modules.php?name=News&file=article&sid=3
3. А. Лукацкий, “Безопасность технологии GPRS”, *Мобильные системы, №2, 2003* http://www.security.strongdisk.ru/i/138&all=1/
4. Mirov, “GPRS уязвимости”, http://www.dataexpress.ru/journal/7.php