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

Технология GPRS и безопасность передачи данных

Никитин Н.И.

07.04.2005

Технология GPRS и безопасность передачи данных

В современном мире едва ли найдётся человек, не взаимодействующий в той или иной степени с электронными устройствами. Причём мобильные устройства, такие как сотовые телефоны, переносные и карманные компьютеры, всё больше входят в нашу жизнь, становясь её неотъемлемой частью и наделяя повседневным удобством. Безусловно, важнейшим является вопрос взаимодействия переносных устройств между собой и создания беспроводных сетей. Наука и быстро развивающаяся техника представляют немалый ряд интересных теоретических решений, однако на практике используемых стандартов, протоколов и решений оказывается не так уж и много. А связано это в первую очередь с достаточной надёжностью и безопасностью системы обработки и передачи данных при её относительно недорогой реализации.

Одним из решений, широко применяемых сегодня в сетях сотовой связи и обеспечивающих обмен данными между мобильными устройствами, является технология пакетной передачи данных GPRS (General Packet Radio Service). Стандарт реализован в подавляющем большинстве современных мобильных аппаратов и имеет ряд достоинств по сравнению с ранее использовавшейся технологией CSD (Circuit Switched Data), предоставляющей доступ в Интернет с мобильных устройств. Основным достоинством является отсутствие постоянной занятости канала передачи данных. После установления соединения с GPRS-узлом, терминал (в частности, мобильный телефон) нагружает линию при непосредственном процессе передачи информации, а не в течение всего времени соединения. Таким образом, ресурсы сети являются распределёнными между всеми подключёнными к системе абонентами. Всвязи с этим пропускная способность системы обслуживания значительно повышается (увеличивается число возможных подключённых к GPRS-сети абонентов в каждый момент времени), а абонент в свою очередь приобретает возможность оплачивать только передаваемый трафик. Другим достоинством технологии является существенно более высокая скорость передачи данных. Если в технологии CSD скорость передачи информации составляла 9,6 Кбит/с, то предел GPRS определяется несомненно более высоким показателем: 171,2 Кбит/с.

Но при появлении новой технологии сразу же возникает вопрос, насколько хорошо является она защищённой от внешних воздействий и попыток препятствовать авторизованному и безопасному процессу передачи информации. Для уяснения возможных проблем в обеспечении информационной безопасности GPRS и методов их решения обратимся к схеме основных компонентов системы, дающей необходимое нам представление об архитектуре GPRS (Рис.1):

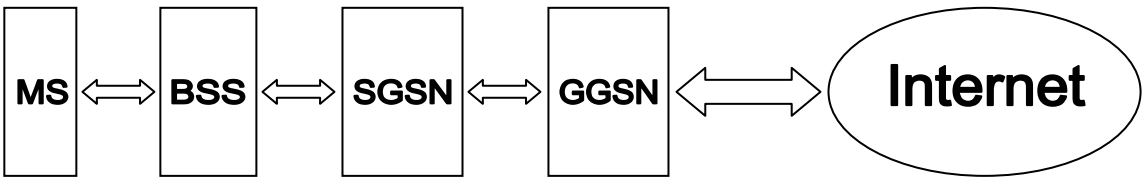

Рис. 1. Схема компонентов GPRS-сети

Не вдаваясь в детали построения, введём следующую простую терминологию элементов сети, удобную для представления сетевой архитектуры:

1. **Мобильная станция** MS (Mobile Station). Представляет собой собственно переносное устройство, состоящее необходимо из 2х элементов:

    - GPRS-модем, осуществляющий приём и передачу информации из сети
    - Терминал, осуществляющий обработку принятой информации

    Как пример, мобильный телефон включает в себя обе вышеуказанные сущности.

2. **Базовая станция** BSS (Base Station System). Базовая станция является промежуточным узлом между мобильной станцией обслуживающим узлом SGSN. BSS определяется однозначно для географической точки нахождения мобильной станции и является ответственной за коммутацию между мобильной станцией и обслуживающим узлом.

3. **Обслуживающий узел** SGSN (Serving GPRS Support Node). SGSN – основной компонент GPRS-сети. Именно обслуживающий узел ответственен за приём, отправку и обработку пакетов от мобильной станции (переданных через коммутацию с базовой станцией). В этом узле происходит шифрование данных. Также узел производит аутентификацию и работу с абонентами сети.

4. **Узел маршрутизации** GGSN (Gateway GPRS Support Node). GGSN по сути является маршрутизатором, ответственным за обмен информацией с внешними GPRS-сетями и Интернетом.

Исходя из вышеуказанного представления о сети, выделим участки, интересные для нашего рассмотрения с точки зрения обеспечения безопасности системы в целом. Нас будут интересовать вопросы безопасности мобильной станции, её соединения с узлом обслуживания и безопасность данных при передаче их по GPRS-сети. К рассмотрению этих вопросов мы вернёмся чуть позже, а пока бы хотелось отметить ещё крайне важный момент в обеспечении безопасности сети – это безопасность при обмене информацией с другими GPRS-сетями и Интернетом. Дело в том, что этот вопрос является одним из самых слабых мест в обеспечении безопасной передачи информации. При взаимодействии с внешними сетями технология предусматривает использование стандартных приёмов обеспечения безопасности в компьютерных сетях. А это подразумевает, что каждый оператор GPRS-сети должен следить за безопасностью взаимодействия с внешними сетями собственноручно и желаемым для него образом. Таким образом, вся ответственность обеспечения защищённости узлов GGSN (а именно они являются взаимодействующими с внешними сетями), ложится на оператора и лишь от его выбора средств защиты сети и качества поддержки и контроля этих средств зависит защищённость передаваемых данных. В силу разных мнений и подходов к организации сетей у различных операторов, в этом месте технологии отсутствует единый стандарт, что всегда даёт большую вероятность разногласий и ошибок при взаимодействии сетей операторов. Это одна из важнейших причин, по которой защищённость информации в GPRS-сетях считается недостаточно надёжной, хотя непосредственно алгоритмы шифрования передаваемых по сети данных реализованы с большой степенью надёжности. К ним мы и перейдём далее.

Отметим вкратце защищённость передачи данных внутри GPRS-сети, а точнее между обслуживающим и узлом маршрутизации (защита информации при передаче между другими компонентами сети реализована иным образом). Для обмена данными между SGSN и GGSN существует протокол GTP (GPRS Tunneling Protocol). Он включает в себя

любые пользовательские протоколы (например, FTP, HTTP итп), а передаваемая информация по умолчанию не шифруется. Однако все внутренние сетевые элементы используют частные IP-адреса, что запрещает пользователям из внешних сетей получать доступ непосредственно к элементам сети и соответственно является защитой передаваемым данным.

Перейдём, наконец, к рассмотрению обеспечения безопасности мобильной станции и её соединения с обслуживающим узлом. Мобильная станция (в частности, мобильный телефон) необходимо имеет **модуль идентификации абонента – SIM-карту**. Функции SIM-карты – это обеспечение аутентификации абонента и мобильной станции в GPRS-сети. Рассмотрим информацию, содержащуюся на карте с целью обеспечения её функциональности:

1. **PIN-код** (Personal Identification Number) для доступа к самой карте.
2. **Идентификатор IMSI** (International Mobile Subscriber Identity), который идентифицирует абонента в сети (уникален для данного абонента и сети).
3. **Ключ аутентификации абонента Ki**. Данный ключ является уникальным для абонента, его длина составляет 128 бит.

Также на карте присутствуют **алгоритмы A3** и **A8**. Алгоритм A3 ответственен за **аутентификацию абонента в сети**. По индивидуальному ключу абонента Ki и некому случайному числу RAND длиной 128 бит, присылаемому сетью в момент соединения, алгоритм должен выработать ожидаемый сетью отклик SRES. Если выработанное алгоритмом значение SRES принимается сетью, то в действие вступает **алгоритм генерации ключей** A8. Алгоритм A8 использует те же индивидуальный ключ абонента Ki и случайное число RAND для генерации 64-битного ключа шифрования Kc, который впоследствии используется мобильной станцией для шифрования данных, передаваемых на узел обслуживания.

Рассмотрим подробнее реализацию алгоритмов A3 и A8. Для этого обратимся к следующей наглядной схеме (Рис.2), на которой представлена функциональность данных двух алгоритмов:

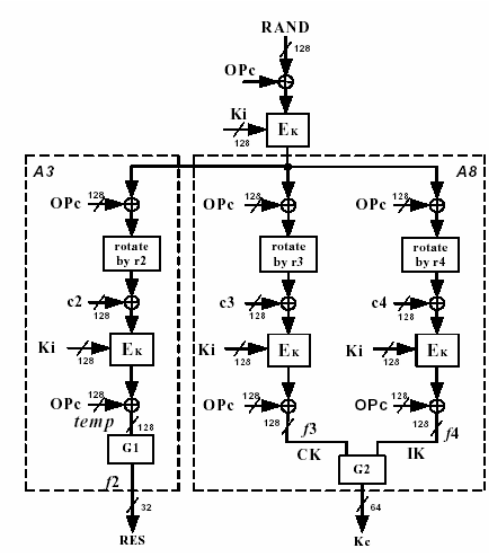

Рис. 2. Схема реализации алгоритмов A3 и A8

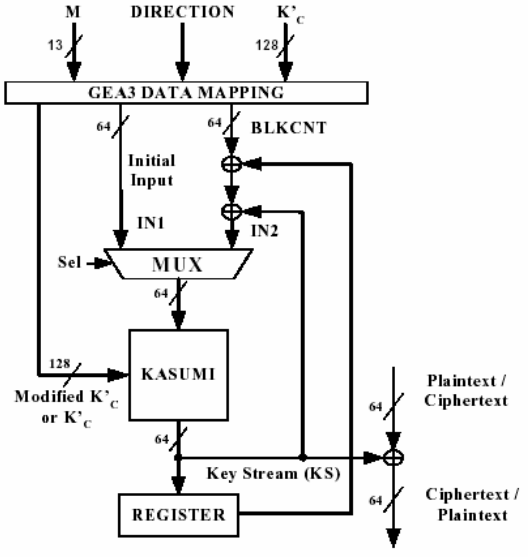

Рис. 3. Схема реализации алгоритма GEA3

Как упоминалось выше, оба алгоритма используют в качестве входных данных значения RAND и Ki. Кроме того, алгоритмы используют ряд определённых констант, задаваемых оператором и хранимых на SIM-карте – OP, ri, ci. OP представляет собой 128-битный вектор предварительных настроек алгоритма, который оператор предпочитает держать в секрете. А потому, при работе алгоритмов используется шифрованный вектор OPc того же размера, получаемый из вектора OP применением шифра Рейндолла (RIJNDAEL) с ключом Ki. Процесс шифрования с помощью шифра Рейндолла обозначен на схеме как Ek. Потому и для векторов настроек справедливо следующее соотношение: OPc = Ek (OP). Итак, алгоритмы A3 и A8 в своей реализации используют так называемые MILENAGE-функции f2, f3 и f4, широко используемые в алгоритмах защиты GSM, UMTS и прочих беспроводных сетей. Каждая fi представляет собой операцию XOR с вектором OPc, затем вращение на константу ri, последующее кодирование с помощью Рейндолл-шифра с ключом Ki и снова операцию XOR с вектором OPc. Таким образом, на выходе функции f2 мы имеем некоторый сигнал (назовём его temp), по которому и происходит вычисление ожидаемого отклика сети SRES по следующему правилу: 64 младших бита сигнала temp делятся на две группы по 32 бита и между ними осуществляется операция XOR. 32-битный SRES и является выходом алгоритма аутентификации A3. Функции же f3 и f4 алгоритма A8 генерируют ключи CK (ciphering key) и IK (integrity key) соответственно, каждый размером 128 бит, которые используются для генерации ключа шифрования Kc следующим образом:

Kc = (CK [0 .. 63]) XOR (CK [64 .. 127]) XOR (IK [64 .. 127]) XOR (IK [64 .. 127]).

Таким образом, после отработки алгоритмов аутентификации A3 и генерации ключа шифрования A8 мобильная станция получает в своё распоряжение значения SRES и Kc.

До сих пор мы вели рассуждения относительно системы безопасности и алгоритмов, реализованных в SIM-карте, рассмотрим же далее вопрос безопасности самого мобильного аппарата. Защита мобильного аппарата обеспечивается хранимым в программном обеспечении аппарата кода **IMEI** (International Mobile Equipment Identity), а также **алгоритмом шифрования** передаваемых на обслуживающий узел данных. Код IMEI персонализирует сам мобильный аппарат и позволяет оператору проверять легальность аппарата, используя хранимые у оператора списки «чёрных» IMEI-кодов (например, краденых телефонов итп). Что касается алгоритма шифрования передаваемых данных, именно он также обеспечивает и безопасность соединения мобильной станции и обслуживающего узла. Обратимся к нему подробнее.

В поздних реализациях GPRS-сетей для шифрования передаваемых от станции к обслуживающему узлу данных используется последняя версия алгоритма семейства A5, а точнее её модификация для GPRS-сетей, - **алгоритм GEA3**. Данный алгоритм использует в качестве ключа шифрования ключ Kc, выработанный ранее алгоритмом A8. Обратим внимание на то, что ровно как и мобильная станция, обслуживающий узел сети оператора имеет значения ключа Ki, а также сгенерированного системой случайного числа RAND (то есть всех входных данных алгоритма A8) и, таким образом, может выработать ключ Kc, используемый для дешифрации получаемых от мобильной станции данных. Для того, чтобы зашифрованный и дешифрованный потоки совпадали, их необходимо синхронизовать. Для этого при передаче обслуживающим узлом мобильной станции сообщения об авторизации, узел сообщает также и некоторые дополнительные параметры синхронизации.

Итак, приступим непосредственно к описанию алгоритма GEA3. Схема реализации GEA3 представлена на рисунке 3. Ядром алгоритма является шифр Казуми (KASUMI), основанный на схеме Фейстеля. Сам же GEA3 является потоковым шифром, кодирующим

блоки данных размером до 64 Кбайт. На вход алгоритм принимает ключ Kc и некоторые дополнительные параметры, задаваемые оператором: Direction, Input, CA, CB и CE. 64-битный ключ Kc расширяется до 128-битного ключа K'c по простому правилу: старшие и младшие 64 разряда ключа K'c образуются копированием в них ключа Kc: K'c = Kc || Kc. Входные параметры используются для создания начального состояния (Initial Input), подаваемого на шифр Казуми. Далее, с использованием ключа K'c шифром Казуми в цикле происходит выработка ключа непосредственного шифрования данных KS (Key Stream), который посредством применения операции XOR к открытому текстом и вырабатывает шифрованный текст. Итерирование по циклу происходит с помощью инкремента переменной BLKCNT.

Поговорим подробнее о реализации алгоритма шифрования Казуми. Для более наглядного представления воспользуемся схемой реализации шифра (Рис.4):

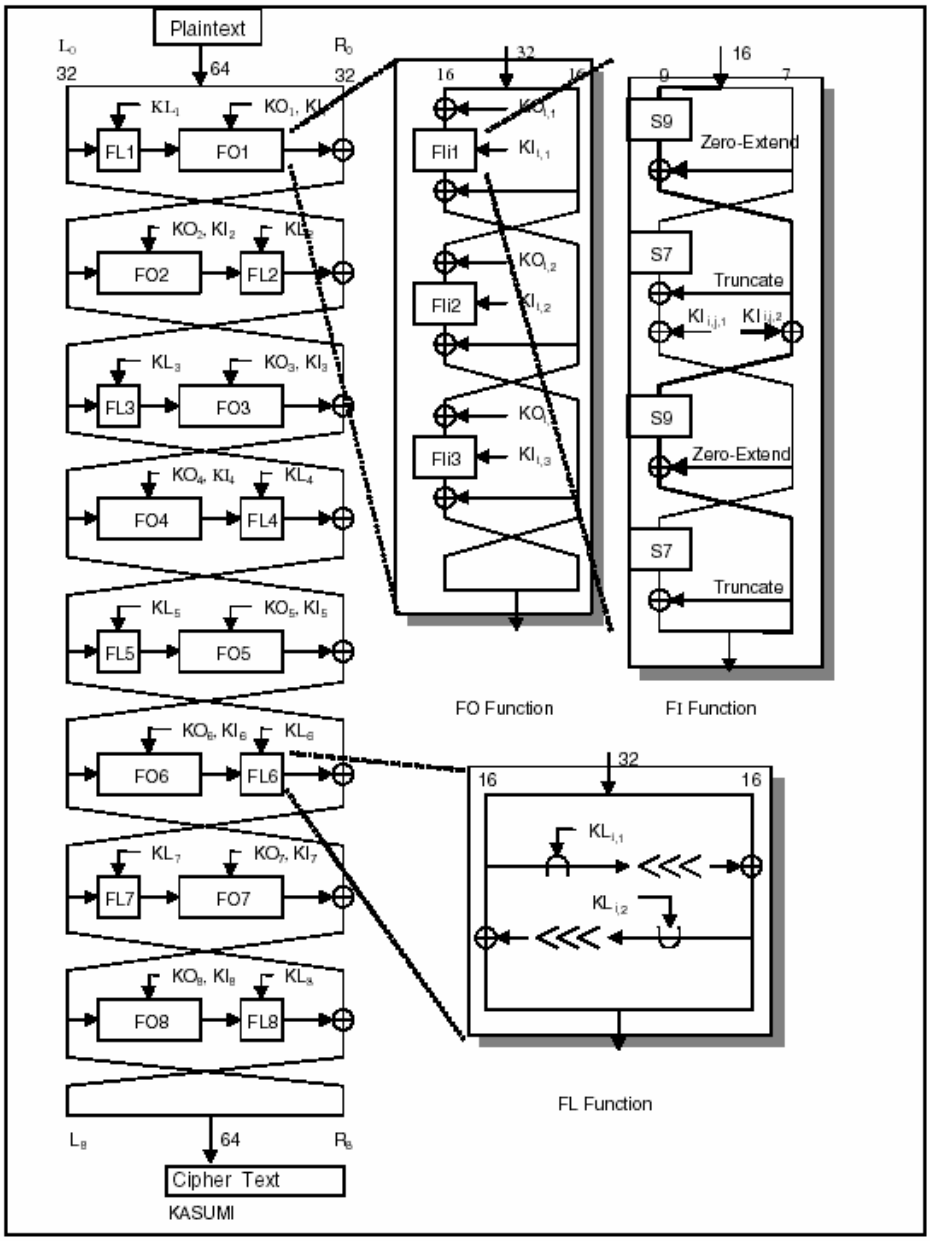

Рис. 4. Схема реализации шифра Казуми (KASUMI)

Как уже упоминалось, данный шифр является шифром Фейстеля с восьмью раундами. В качестве входных данных используются 128-битный ключ K и строка S. Входная строка делится на правую R_0 и левую L_0 части, равные по 32 бита каждая. На каждом из восьми раундов обе части преобразуются по следующему правилу:

$$R_i = L_{i-1}; \quad L_i = R_{i-1} \quad \text{XOR} \quad f(L_{i-1}, RK_i),$$

где fi определяет функцию раунда, принимающую в качестве аргументов ключ раунда RK_i и 32-битное входное значение. Ключ раунда RK_i состоит реально из трёх ключей KL_i, KO_i и KI_i, за генерацию которых ответственен элемент распределения ключей (key Scheduling Unit). Функция fi состоит из трёх функций FL, FO и FI, которые и используют 3 соответствующих ключа. Итак,

- Функция FL принимает 32-битный входной параметр и с помощью 32-битного ключа KL_i генерирует выход также размерности 32 бита.
- Функция FO принимает 32-битный входной параметр и два 48-битных ключа KO_i и KI_i. Последний используется при вызове функции FI.
- Функция FI принимает 16-битный входной параметр и 16-битный ключ $KI_{i,j}$ и генерирует на их основе 16-битный выход.

Из схемы нетрудно выяснить, какие логические операции использует каждая из этих функций. Стоит лишь отметить, что функция FI использует S-box'ы S7 и S9, осуществляющие преобразования входных 7ми и соответственно 9ти бит в выходные 7 и 9 бит. Легко также сделать вывод, что сама функция fi имеет определённый вид (порядок выполнения функций FL и FO) в зависимости от чётности раунда. Так, на нечётных раундах первой исполняется функция FL, а на чётных – FO.

Итак, сгенерированный алгоритмом Казуми ключ выдаётся впоследствии алгоритмом GEA3 и используется для кодирования данных, транслируемых между мобильной станцией и обслуживающим узлом.

Таким образом, мы рассмотрели архитектуру GPRS-сети, её базовые компоненты, механизмы и их защиты и некоторые реализованные алгоритмы, и, наконец, возможные места уязвимости с точки зрения информационной безопасности. Однозначный вывод о надёжности защиты технологии сделать непросто, как и создать совершенную систему защиты. Более того, создатели тех или иных механизмов безопасности зачастую утверждают об их стопроцентной надёжности, однако через некоторое время эти механизмы объявляются взломанными. Но стоит отметить и тот факт, что отсутствие явной стандартизации зачастую приводит к проблемам, связанным с безопасностью системы в целом. Потому, можно лишь говорить о достаточной надёжности защиты на сегодняшний день вплане повседневного использования технологии.

Литература:

1. **“Безопасность технологии GRPS”.**
   Алексей Лукацкий, 2003
   http://www-old.infosec.ru/press/pdf/p151.pdf

2. **“An End-to-End Hardware Approach Security for the GPRS”.**
   P. Kitsos, N. Sklavos, O. Koufopavlou, 2004
   http://www.vlsi.ee.upatras.gr/~pkitsos/Kitsos_melecon04.pdf

3. **“KASUMI Block Cipher on the StarCore SC140 Core”.**
   Mao Zeng, 2004
   http://www.freescale.com/files/dsp/doc/app_note/AN2837.pdf

4. **“Security Mechanisms in UMTS”.**
   Stefan Pütz, Roland Schmitz, Tobias Martin, 2001
   http://fb1.hdm-stuttgart.de/skripte/Internetsecurity_2/Papers/UMTS-SecurityMechanisms.pdf

5. **“Cryptographic Algorithms for UMTS”.**
   P. Neittaanmäki, T. Rossi, S. Korotov, E. Oñate, J. Périaux, and D. Knörzer (eds.), 2004
   http://www.tcs.hut.fi/Studies/T-79.159/articles/nyberg.pdf