Алексеев Г. 914гр.

БЕЗОПАСНОСТЬ В СТАНДАРТЕ СОТОВОЙ СВЯЗИ GSM

В стандарте GSM термин "безопасность" понимается как исключение несанкционированного использования системы и обеспечение секретности переговоров подвижных абонентов. Определены следующие механизмы безопасности в стандарте GSM [2]:

- аутентификация;

- секретность передачи данных;

- секретность абонента;

- секретность направлений соединения абонентов.

Защита сигналов управления и данных пользователя осуществляется только по радиоканалу. Режимы секретности в стандарте GSM определяются Рекомендациями, приведенными в таблице 1.

Таблица 1

GSM 02.09	Аспекты секретности	Определяет характеристики безопасности, применяемые в сетях GSM. Регламентируется их применение в подвижных станциях и сетях
GSM 03.20	Секретность, связанная с функциями сети	Определяет функции сети, необходимые для обеспечения характеристик безопасности, рассматриваемых в рекомендациях GSM 02.09
GSM 03.21	Алгоритмы секретности	Определяет криптографические алгоритмы в системе связи
GSM 02.17	Модули подлинности абонентов (SIM)	Определяет основные характеристики модуля SIM

Рассмотрим последовательно механизмы безопасности в стандарте GSM, общий состав секретной информации, а также ее распределение в аппаратных средствах GSM системы. При этом будем использовать термины и обозначения, принятые в рекомендациях GSM.

1. Механизмы аутентификации

Для исключения несанкционированного использования ресурсов системы связи вводятся и определяются механизмы аутентификации - удостоверения подлинности абонента. Каждый подвижный абонент на время пользования системой связи получает стандартный модуль подлинности абонента (SIM-карту), который содержит:

- международный идентификационный номер подвижного абонента (IMSI);

- свой индивидуальный ключ аутентификации (Ki);

- алгоритм аутентификации (A3).

С помощью заложенной в SIM информации в результате взаимного обмена данными между подвижной станцией и сетью осуществляется полный цикл аутентификации и разрешается доступ абонента к сети.

Процедура проверки сетью подлинности абонента реализуется следующим образом. Сеть передает случайный номер (RAND) на подвижную станцию. Подвижная станция определяет значение отклика (SRES), используя RAND, Ki и алгоритм A3:

```
SRES = Ki [RAND]
```

Подвижная станция посылает вычисленное значение SRES в сеть, которая сверяет значение принятого SRES со значением SRES, вычисленным сетью. Если оба значения совпадают, подвижная станция может осуществлять передачу сообщений. В противном случае связь прерывается, и индикатор подвижной станции должен показать, что опознавание не состоялось.

По причине секретности вычисление SRES происходит *в* рамках SIM. Несекретная информация (такая как Ki) не подвергается обработке в модуле SIM. Процедура аутентификации иллюстрируется рис.1.

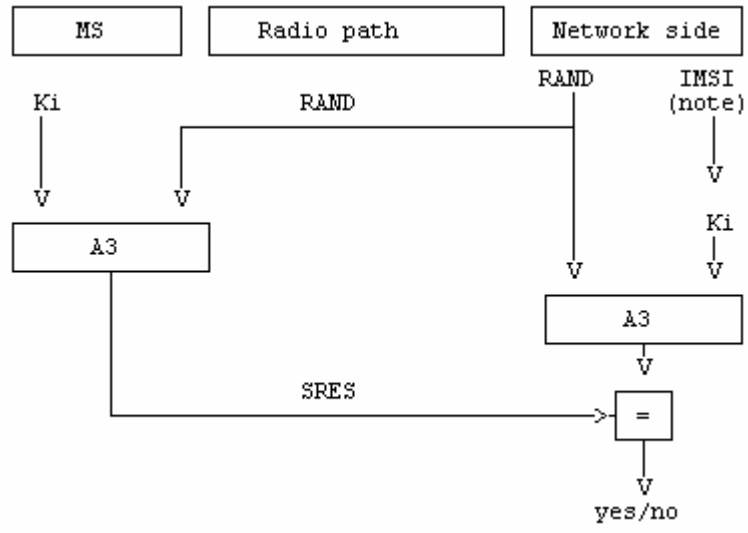

Рис.1. Аутентификация подвижной станции.

2. Секретность передачи данных

Ключ шифрования

Для обеспечения секретности передаваемой по радиоканалу информации вводится следующий механизм защиты. Все конфиденциальные сообщения должны передаваться в режиме защиты информации. Алгоритм формирования

ключей шифрования (A8) хранится в модуле SIM. После приема случайного номера RAND подвижная станция вычисляет, кроме отклика SRES, также и ключ шифрования (Кс), используя RAND, Ki и алгоритм A8 (рис. 2):

Кс = Ki [RAND].

Ключ шифрования Кс не передается по радиоканалу. Как подвижная станция, так и сеть вычисляют ключ шифрования, который используется другими подвижными абонентами. По причине секретности вычисление Кс происходит в SIM.

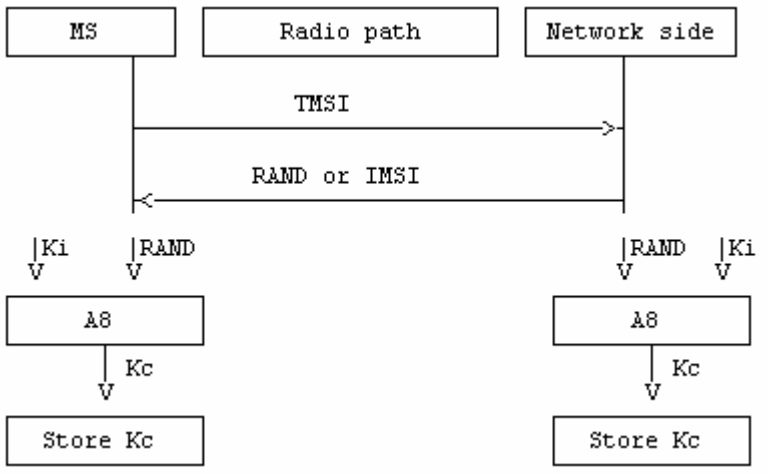

Рис.2. Генерация ключа шифрования.

Числовая последовательность ключа шифрования

Кроме случайного числа RAND сеть посылает подвижной станции числовую последовательность ключа шифрования. Это число связано с действительным значением Кс и позволяет избежать формирование неправильного ключа. Число хранится подвижной станцией и содержится в каждом первом сообщении, передаваемом в сеть. Некоторые сети принимают решение о наличии числовой последовательности действующего ключа шифрования в случае, если необходимо приступить к опознаванию или, если выполняется предварительное опознавание, используя правильный ключ шифрования. В некоторых случаях это допущение реально не обеспечивается.

Установка режима шифрования

Для установки режима шифрования сеть передает подвижной станции команду CMC (Ciphering Mode Command) на переход в режим шифрования. После получения команды CMC подвижная станция, используя имеющийся у нее ключ, приступает к шифрованию и дешифрованию сообщений. Поток передаваемых данных шифруется бит за битом или поточным шифром, используя алгоритм шифрования A5 и ключ шифрования Кс.

3. Обеспечение секретности абонента

Для исключения определения (идентификации) абонента путем перехвата сообщений, передаваемых по радиоканалу, каждому абоненту системы связи присваивается "временное удостове рение личности" - временный

международный идентификационный номер пользователя (TMSI), который действителен только в пределах зоны расположения (LA). В другой зоне расположения ему присваивается новый TMSI. Если абоненту еще не присвоен временный номер (например, при первом включении подвижной станции), идентификация проводится через международный идентифи кационный номер (IMSI). После окончания процедуры аутентификации и начала режима шифрования временный идентификационный номер TMSI передается на подвижную станцию только в зашифрованном виде. Этот TMSI будет использоваться при всех последующих доступах к системе Если подвижная станция переходит в новую область расположения, то ее TMSI должен передаваться вместе с идентификационным номером зоны (LAI), в которой TMSI был присвоен абоненту.

4. Обеспечение секретности в процедуре корректировки местоположения

При выполнении процедуры корректировки местоположения по каналам управления осуществляется двухсторонний обмен между MS и BTS служебными сообщениями, содержащими временные номера абонентов TMSI. В этом случае в радиоканале необходимо обеспечить секретность переименования TMSI и их принадлежность конкретному абоненту.

Рассмотрим, как обеспечивается секретность в процедуре корректировки местоположения в случае, когда абонент проводит сеанс связи и при этом осуществляет перемещение из одной зоны расположения в другую.

В этом случае подвижная станция уже зарегистрирована в регистре перемещения VLR с вре менным номером TMSI, соответствующим прежней зоне расположения. При входе в новую зону расположения осуществляется процедура опознавания, которая проводится по старому, зашифрованному в радиоканале TMSI, передаваемому одновременно с наименованием зоны расположени LAI. LAI дает информацию центру коммутации и центру управления о направлении перемещени подвижной станции и позволяет запросить прежнюю зону располбжения о статусе абонента и его данные, исключив обмен этими служебными сообщениями по радиоканалам управления. При этом по каналу связи передается как зашифрованный информационный текст с прерыванием сообщения в процессе “эстафетной передачи” на 100-150 мс.

5. Общий состав секретной информации и ее распределение в аппаратных средствах GSM

В соответствии с рассмотренными механизмами безопасности, действующими в стандарте GSM, секретной считается следующая информация: RAND - случайное число, используемое для аутентификации подвижного абонента;

- значение отклика - ответ подвижной станции на полученное случайное число;

- индивидуальный ключ аутентификации пользователя, используемый для вычисления значения отклика и ключа шифрования;

- ключ шифрования, используемый для шифрования/дешифрования сообщений, сигналов управления и данных пользователя в радиоканале;

- алгоритм аутентификации, используемый для вычисления значения отклика из случайного числа с использованием ключа Ki;

- алгоритм формирования ключа шифрования, используемый для вычисления ключа Кс из случайного числа с использованием ключа Ki;

- алгоритм шифрования/дешифрования сообщений, сигналов управления и данных пользователя с использованием ключа Кс;

- номер ключевой последовательности шифрования, указывает на действительное число Кс, чтобы избежать использования разных ключей на передающей и приемной сторонах;

- временный международный идентификационный номер пользователя.

В таблице 2 показано распределение секретной информации в аппаратных средствах системы связи GSM.

Таблица 2.

Номер	Аппаратные средства	Вид секретной информации
1	Подвижная станция (без SIM)	A5
2	Модуль подлинности абонента (SIM)	A3; A8; IMSI; Ki; TMSI/LAI; Kc/CKSN
3	Центр аутентификации (AUC)	A3; A8; IMSI/Ki
4	Регистр местоположения (HLR)	Группы IMSI/RAND/SRES/Kc
5	Регистр перемещения (VLR)	Группы IMSI/RAND/SRES/Kc, IMSI/TMSI/LAI/Kc/CKSN
6	Центр коммутации (MSC)	A5; TMSI/IMSI/Kc
7	Контроллер базовой станции (BSC)	A5; TMSI/IMSI/Kc

6. Обеспечение секретности при обмене сообщениями между HLR, VLR и MSC

Основным объектом, отвечающим за все аспекты безопасности, является центр аутентификации (AUC). Этот центр может быть отдельным объектом или входить в состав какого-либо оборудования, например, в регистр местоположения (HLR). Как управлять AUC будет решать тот, кому будет поручена эксплуатация сети. Интерфейс GSM с AUC не определен.

AUC может решать следующие задачи:

- формирование индивидуальных ключей аутентификации пользователей Ki и соответствующих им международных идентификационных номеров абонентов (IMSI);

- формирование набора RAND/SRES/Kc для каждого IMSI и раскрытие этих групп для HLR при необходимости.

Если подвижная станция переходит в новую зону расположения с новым VLR, новый VLR должен получить секретную информацию об этой подвижной станции. Это может быть обеспечено следующими двумя способами:

- подвижная станция проводит процедуру идентификации по своему международному номеру IMSI. При этом VLR запрашивает у регистра местоположения HLR группы данных RAND/SRES/Kc, принадлежащих данному IMSI;

- подвижная станция проводит процедуру аутентификации, используя прежний временный номер TMSI с наименованием зоны расположения LAI. Новый VLR запрашивает прежний VLR для посылки международного номера IMSI и оставшихся групп из RAND/SRES/Kc, принадлежащих этим TMSI/LAI,

Если подвижный абонент остается на более длительный период в VLR, тогда после некоторого количества доступов с аутентификацией VLR из соображений секретности потребует новые группы RAND/SRES/Kc от HLR.

Все эти процедуры определены в рекомендации GSM 09.02.

Проверка аутентификации выполняется в VLR. VLR посылает RAND на коммутационный центр (MSC) и принимает соответствующие отклики SRES. После положительной аутентификации TMSI размещается с IMSI. TMSI и используемый ключ шифрования Kc посылаются в центр коммутации (MSC). Эти же процедуры определяются в рекомендации GSM 09.02.

Передача секретной информации по радиоканалу уже описана в предыдущих разделах и определена в рекомендации GSM 04.08.

7. Модуль подлинности абонента

Введение режима шифрования в стандарте GSM выдвигает особые требования к подвижным станциям, в частности, индивидуальный ключ аутентификации пользователя Ki, связанный с международным идентификационным номером абонента IMSI, требует высокой степени защиты. Он также используется в процедуре аутентификации.

Модуль подлинности абонента SIM содержит полный объем информации о конкретном абоненте. SIM реализуется конструктивно в виде карточки с встроенной электронной схемой. Введение SIM делает подвижную станцию универсальной, так как любой абонент, используя свою личную SIM-карту, может обеспечить доступ к сети GSM через любую подвижную станцию.

Несанкционированное использование SIM исключается введением в SIM индивидуального идентификационного номера (PIN), который присваивается пользователю при получении разрешения на работу в системе связи и регистрации его индивидуального абонентского устройства.

Основные характеристики модуля SIM определены в Рекомендации GSM 02.17. Состав секретной информации, содержащейся в SIM, показан в таблице 2.

В заключение следует отметить, что выбранные в стандарте GSM механизмы секретности и методы их реализации определили основные элементы передаваемых информационных блоков и направления передачи, на которых должно осуществляться шифрование: (RAND/SRES/Kc от HLR к VLR; RAND и SRES - в радиоканале). Для обеспечения режима секретности в стандарте GSM решены вопросы минимизации времени соединения абонентов. При организации систем сотовой радиосвязи по стандарту GSM имеется некоторая свобода в применении аспектов безопасности. В частности, не стандартизованы вопросы использования центра аутентификации AUC (интерфейс с сетью, структурное размещение AUC в аппаратных средствах). Нет строгих рекомендаций на формирование закрытых групп пользователей и системы приоритетов, принятых в GSM. В этой связи в каждой системе связи, использующей стандарт GSM, эти вопросы решаются самостоятельно.

Система безопасности в GSM в конетексте других стандартов сотовой связи.

С самого начала страндарт GSM преподносился как исключительно безопасный. Однако впоследствии стало ясно, не все были заинтересованы в «неуязвимости» стандарта. Анализируя алгоритмы A5 и A3/A8 можно прийти к выводу, что их стойкость могла бы быть существенно выше за счет очевидных незначительных усовершенствований (например, увеличение длины регистров сдвига в алгоритме A5). В настоящее время все алгоритмы взломаны, и существуют программно-аппратные комплексы, позволяющие в режиме реального времени прослушивать чужие разговоры. Так, например, для персонального компьютера средней конфигурации (Pentium II, 500MHz) с соотетвтвующим программным обеспечением требуется около двух минут анализа закодированного трафика, после чего его расшифровка занимает менее секунды.

Тем не менее, сложность перехвата сообщений (а следовательно и стоимость оборудования) стандарта GSM существенно выше, чем аналоговых стандартов NMT-450/900, AMPS, TACS. Последние практически никак не защищают передаваемые данные, и для перехвата необходим лишь радиосканер. В аналоговых стандартах вся система безопасности сводится в лучшем случае к обеспечению подлинности подвижной станции.

Другое дело – CDMA. Коротко говоря, в этом стандарте конфиденциальность связи максимальная из всех технологий подвижной связи. Это обусловлено типом используемого радиосигнала с широкой базой D=BT=100, где D - база или коэффициент сжатия сигнала, B (МГц) - полоса сигнала cdmaOne в эфире, а T (мксек) - длительность информационной посылки. Обнаружить сам факт наличия такого сигнала специальными средствами в эфире гораздо сложнее, чем "простых" узкополосных сигналов, используемых в стандартах GSM, DAMPS, NMT, поскольку спектральная плотность мощности сигнала cdmaOne в эфире на получается 20дБ ниже при равных скоростях передачи информации и мощности передатчика. Следует попутно отметить, что именно благодаря использованию такого "широкобазового" типа сигнала в радиоинтерфейсе технологии CDMA обеспечивается максимальная надежность связи в условиях многолучевых замираний по сравнению с технологиями стандартов GSM, DAMPS, NMT. Наивысшая конфиденциальность связи обусловлена многоступенчатым кодированием, расшифровка которого потребует попросту нескольких весьма напряженных лет упорного труда. Так, если сигналы аналоговых стандартов можно прослушать самыми простыми измерительными приемниками, которые свободно продаются в магазинах, то для прослушивания с эфира сигналов сигналов стандартов GSM и DAMPS поставляется уже более совершенная аппаратура радиоконтроля.

В рамках перехода к беспроводным сетям третьего поколения, которые обещают быть более унифицированными с точки зрения стандартов и спецификаций, разрабатываются также новые, более совершенные методы защиты, включающие в себя защиту подлинности абонента, аутентификацию и защиту передаваемых данных. Большое количество технической информации на эту тему доступно на сайте организации 3GPP.

Приложение.

1. Описание алгоритма A5.

Алгоритм описан в стандарте GSM 03.20. Используется для шифрования голосовых данных и конфеденциальных сигнальных сообщений на участке подвижная станция – базовая станция. На всем остальном участке транспортной сети трафик остается незашифрованным.

Существует в модификации алгоритма: A5/2, и с повышенной стойкостью - A5/1. Последний запрещен для использования в «третьих» странах.

Генератор A5/2 состоит из трёх РСЛОС длиной 19, 22 и 23, что в сумме и дает 64-битный сеансовый ключ шифрования в GSM. Все многочлены обратной связи у него прорежены. Выходом является результат операции XOR над тремя РСЛОС. В A5 используется изменяемое управление тактированием. Каждый регистр тактируется в зависимости от своего среднего бита, затем над регистром выполняется операция XOR с обратной пороговой функцией средних битов всех трех регистров. Обычно на каждом этапе тактируютя два РСЛОС. Существует тривиальное вскрытие A5/2, требующее 2^{40} шифрований: предпологаем содержание первых двух РСЛОС и пытаемся определить третий РСЛОС по гамме.

В A5/1 добавлен еще один короткий регистр длиной 17 бит, управляющий движением бит в остальных трех регистрах. Для вскрытия системы достаточно лобовым перебором (сложность 216 = 65536 отыскать заполнение управляющего регистра. Делается это всего по двум фреймам сеанса связи длиной по 114 бит (в системе GSM первые два фрейма шифрпоследовательности известны, поскольку шифруются одни нули).

A5- криптосхема на основе регистров сдвига с линейной обратной связью имеет комбинирующий генератор для получения шифрующей последовательности. Поэтому надо использовать слабости в комбинирующей функции, которые позволяют по выходной последовательности получить информацию об отдельных входных последовательностях узла усложнения. В этом случае говорят, что имеется корреляция между выходной последовательностью и одной из внутренних последовательностей. Вследствие такой корреляции отдельная внутренняя последовательность может быть проанализирована индивидуально вплоть до восстановления начального заполнения соответствующего регистра, затем внимание надо переключить на одну из других внутренних последовательностей. Подобным способом может быть восстановлен весь генератор - этот метод часто называют атака "разделяй-и-вскрывай". Причем первым из регистров надо выбрать тот, который проще чем остальные восстановить.

Литература.

1. Брюс Шнайер, «Прикладная криптография».
2. 3rd Generation Partnership Project (3GPP). Спецификация 43.020 архитектуры системы безопасности сетей GSM: http://www.3gpp.org/ftp/Specs/archive/43_series/43.020/
3. Описание аспектов безопасности в стандарте GSM. http://www.aboutphone.info/js/kunegin/gsm/4_1.html