Виды мошенничества в сети GSM и защита от них

Яковлева Надежда

16.04.2004

Введение

Бурное развитие новых телекоммуникационных технологий в 80-90-е годы связано с активным использованием достижений науки и техники в отраслях электросвязи, информационных технологий и электроники. К одной из приоритетных технологий относится сотовая связь, которая завоевывает все большую популярность у населения и развивается весьма быстрыми темпами. И одним из важнейших условий для существования и дальнейшего развития такого вида связи является обеспечение ее безопасности.

Например, в первых аналоговых мобильных сетях обеспечение безопасности находилось на очень низком уровне. В пришедших на смену им цифровых системах GSM и DAMPS менялся характер и уровень обеспечения безопасности, а вместе с ними и характер мошенничества. Нарушителям становилось все труднее и дороже перехватывать информацию и клонировать трубки. Это привело к переходу от технического мошенничества к процедурному и контрактному. Однако, техническое мошенничество все же возможно, так как если перед мошенником закрыта дверь, то он будет пытаться влезть в окно.

По данным мировой статистики, уровень потерь операторов мобильной связи составляет 2-6%, а по данным самих компаний, может доходить до 25%. В Москве же ущерб оценивается в пределах 3 – 5 млн. рублей в месяц (данные предоставлены АО «МГТС»).

Для решения этих задач в сетях GSM и будущих системах UMTS необходимо принимать дополнительные меры безопасности, которые сделают их значительно менее уязвимыми.

Так что же такое мошенничество в сетях мобильной связи? Выделяют следующие способы “обмана”:

Мошенничество (fraud) - неправомочный и преднамеренный доступ абонента к услугам связи с целью личной или коллективной выгоды

Мошеннический доступ (access fraud) - несанкционированное использование услуг связи путем перепрограммирования серийных (ESN, Electronic Serial Number) или (MIN,Mobile Identification Number) идентификационных номеров сотовых телефонов

Мошенничество с украденным телефоном (stolen phone fraud) – использование украденного или потерянного сотового телефона

Контрактное мошенничество (subscription fraud) - преднамеренное указание неверных данных при заключении контракта или невыполнение абонентом контрактных условий оплаты

Хакерское мошенничество (hacking fraud) - проникновение хакеров в компьютерную систему защиты для удаления механизмов защиты или переконфигурации системы в своих целях

Техническое мошенничество (technical fraud) - неправомочное изготовление (клонирование) телефонных трубок или платежных телефонных карт с фальшивыми идентификаторами абонентов, номеров и платежных отметок

Процедурное мошенничество (procedural fraud) - неправомочное использование роуминга и других бизнес-процедур (например, биллинга) с целью уменьшения оплаты услуг связи

Мошенничество с телефонными картами (смарт-картами) - использование слабых мест в процедурах производства, распределения, активизации и вывода из обращения оплаченных телефонных карт

Общая схема перехвата информации в аналоговых стандартах (AMPS и NMT) такова:

1) мошенники перехватывают с помощью сканеров идентифицирующий сигнал чужого телефона, которым он отвечает на запрос базовой станции
2) выделяют из него идентификационные номера MIN и ESN и перепрограммируют этими номерами микрочип своего телефона.

В результате, стоимость разговора с этого аппарата заносится базовой станцией на счет того абонента, у которого эти номера были украдены.

В цифровых же стандартах (GSM и DAMPS) это сделать намного труднее, даже невозможно. Все дело в том, что базовая станция здесь посылает случайный служебный сигнал, а телефон его шифрует и отправляет обратно. Поэтому, даже перехватив сигнал, мошенники не смогут узнать код, дабы хотя бы прослушать разговор абонента.

Также широко известен и популярен метод так называемого «клонирования» телефонов. Клонирование основано на том, что абонент использует чужой идентификационный номер (а, следовательно, и счет) в корыстных целях. Тут абонента даже не спасет сотовая трубка стандарта GSM, если его телефон, SIM-карта (неважно каким способом) попал на некоторое время к мошенникам. Все, что им надо при клонировании трубки, эта сама трубка и всего лишь на несколько часов. Единственное “утешение”, что прослушать разговор абонента все равно будет невозможно; мошенники смогут только звонить за его счет.

Можно взять на заметку следующие проблемы, возникающие при использовании трубок-двойников:

1) когда и мошенник (фрикер), и легальный абонент пытаются произвести звонок одновременно, тот, кто набрал номер первым, может разговаривать свободно, аппарат второго либо не найдет сеть, либо примет сигнал "номер занят".
2) при попытке вместе ответить на входящий вызов оба аппарата сбросят звонок или вообще не будут подавать никаких сигналов.

Нормально пользоваться связью можно только тогда, когда кто-то из двойников находится вне зоны покрытия или качество приема у одной из трубок на порядок выше, чем у другой.

Как же защитить сотовый телефон и работу с ним?

- узнайте у фирмы-производителя, какие средства против мошенничества интегрированы в ваш аппарат;
- держите документы с ESN-номером вашего телефона в надежном месте;

ежемесячно и тщательно проверяйте счета на пользование сотовой связью (это основное);

- в случае кражи или пропажи вашего сотового телефона сразу предупредите фирму, предоставляющую вам услуги сотовой связи;
- держите телефон отключенным до того момента, пока вы не решили им воспользоваться.
- не пользуйтесь стандартами: транковой связи - все они легко взламываются хакерами.

На заметку: с сентября 1995 г. по январь 1999 г. рядом компаний (Vodafone, Siemens, Panafon, Swisscom и др.) разрабатывался совместный проект ASPeCT (Advanced Security for Personal Communication Technologies - Усовершенствованные средства защиты для персональной связи). Но разрабатывался он исключительно для UMTS, как стандарта связи 3-го поколения. Скорее всего существующие цифровые стандарты плавно перетекут в этот пока не очень популярный стандарт связи (на данный момент им пользуются чуть более 60 млн. человек в 30 странах мира, в то время как в России число всех пользователей сотовой связи составило 36млн.), так же как и осуществился переход от аналоговых систем к цифровым, а пока все же перейдем к существующей защите GSM.

Защита GSM

Фундамент системы безопасности GSM составляют три секретных алгоритма(официально не раскрытые и сообщаемые лишь тем кому это требуется для необходимости- операторам связи, поставщикам оборудования.)

A3-алгоритм аутентификации, защищающий телефон от клонирования путем перехвата сообщений.

A8-алгоритм генерации криптоключа, однонаправленная функция, которая берет фрагмент выхода A3 и превращает его в сеансовый ключ A5

A5-алгоритм шифрования оцифрованной речи. В GSM используются две основные разновидности алгоритма: A5/1 и A5/2(используемый и в России). В настоящее время утвержден алгоритм A5/3.

Механизм аутентификации

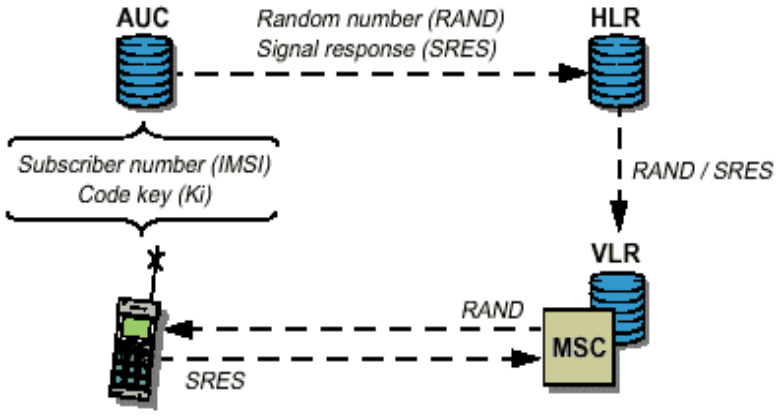
Механизм аутентификации по сути дела является процедурой удостоверения подлинности абонента, для того чтобы исключить несанкционированное использование ресурсов системы связи.

Во время пользования системой связи, телефон абонента получает SIM-карту (так называемый “модуль подлинности абонента”), содержащую номер IMSI (international mobile subscriber identity, то есть международный идентификационный номер подвижного абонента), Ki (subscriber authentication key-индивидуальный ключ аутентификации) и алгоритм аутентификации A3.

Также стоить отметить, что значения IMSI и Ki также хранятся в специальном сегменте сети AUC (центр аутентификации)

Так выглядит схема проверки подлинности абонента сетью:

1) Сегмент AUC генерирует случайный номер RAND и вычисляет значение SRES (signal response), следующим образом: SRES=Ki [RAND]
2) Далее значения SRES и RAND помещаются в сегмент HLR (регистр местоположения)
3) MSC (центр коммутации), используя номер IMSI, достает значения SRES и RAND из HLR и посылает значение RAND на подвижную станцию MS
4) MS определяет значение отклика SRES, используя зашитый в SIM-карту ключ Ki и алгоритм A3, SRES=Ki [RAND. Вычисление отклика происходит в модуле SIM. Затем MS отправляет вычисленное значение обратно в MSC
5) Далее в MSC происходит сверка значений SRES, вычисленного MS и сетью. Если оба значения совпадают, то подвижная станция может осуществлять передачу сообщений. Если же нет, то связь прерывается, а индикатор MS должен показать, что опознавание не состоялось.



VLR – регистр перемещения

Секретность передачи данных

Сам заголовок и означает, что все конфиденциальные сообщения должны передаваться в режиме защиты информации.

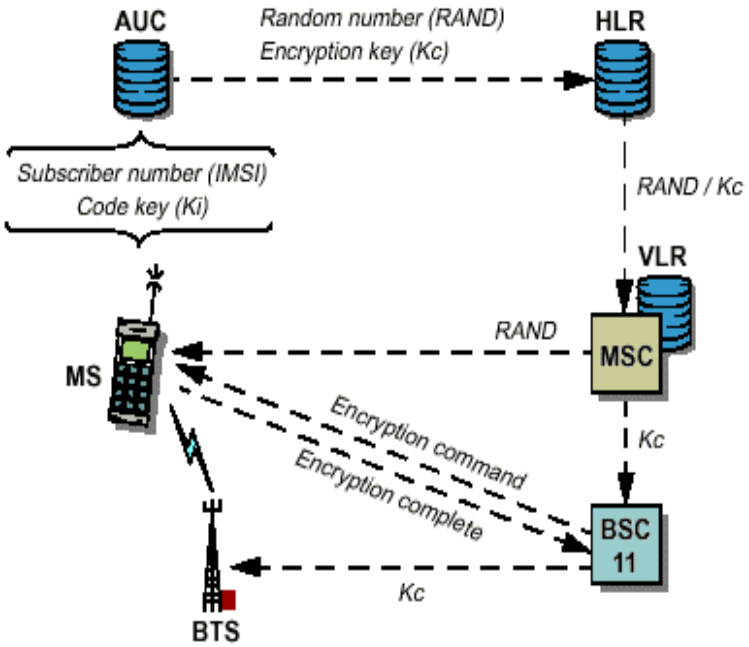
Алгоритм формирования ключей шифрования A8 хранится в модуле SIM.

Наилучшим решением является шифрование внешнего интерфейса, как для канала потока данных, так и для канала управления. Поскольку шифрование голоса требует цифрового кодирования, оно не может быть использовано в аналоговых сетях. Каналы

управления в принципе могут быть зашифрованы в аналоговых и цифровых системах, но шифрование более распространено в мобильных сетях, которые используют цифровые контрольные каналы, такие как GSM и D-AMPS.

В GSM голос шифруется следующим образом:

1) AUC помимо SRES вычисляет также ключ шифрования Kc = Ki [RAND], и также помещается в HLR вместе с RAND и SRES.
2) После приема случайного номера RAND подвижная станция также вычисляет отклик SRES, а также ключ шифрования Kc = Ki [RAND], используя RAND, Ki и алгоритм A8. По причине секретности вычисление Kc происходит в SIM. Ключ шифрования Kc хранится в HLR наряду SRES и RAND.
3) Ключ Kc по каналу связи не передается
4) При положительном прохождении аутентификации MSC заносит ключ шифрования Kc в базовую станцию (или BSC) для использования операций шифрования/расшифрования.
5) Затем BSC посылает подвижной станции MS “тестовый сигнал” (encryption mode command). Этот сигнал связан с действительным значением Kc и позволяет избежать формирование неправильного ключа
6) В ответ MS должна произвести зашифрованный сигнал (encryption mode complete), который (если BSC смогла интерпретировать его) позволяет продолжить соединение: все сигналы с данного момента, включая голосовые данные, шифруются. Поток передаваемых данных шифруется бит за битом или поточным шифром, используя алгоритм шифрования A5 и ключ шифрования Kc.



VLR – регистр перемещения

BSC - контроллер базовой станции

Идентификация оборудования

Цель идентификации оборудования состоит в том, чтобы исключить использование в сети украденных или неавторизованных по другим причинам мобильных телефонов. Для этого каждый сотовый телефон снабжен номером IMEI (international mobile equipment identity). Во время регистрации MSC может потребовать номер IMEI и переслать его для проверки в элемент сети, называемый EIR (в сетях GSM). Если номер является запрещенным или неизвестным, то попытка регистрации отклоняется

Конфиденциальность идентификационного номера абонента

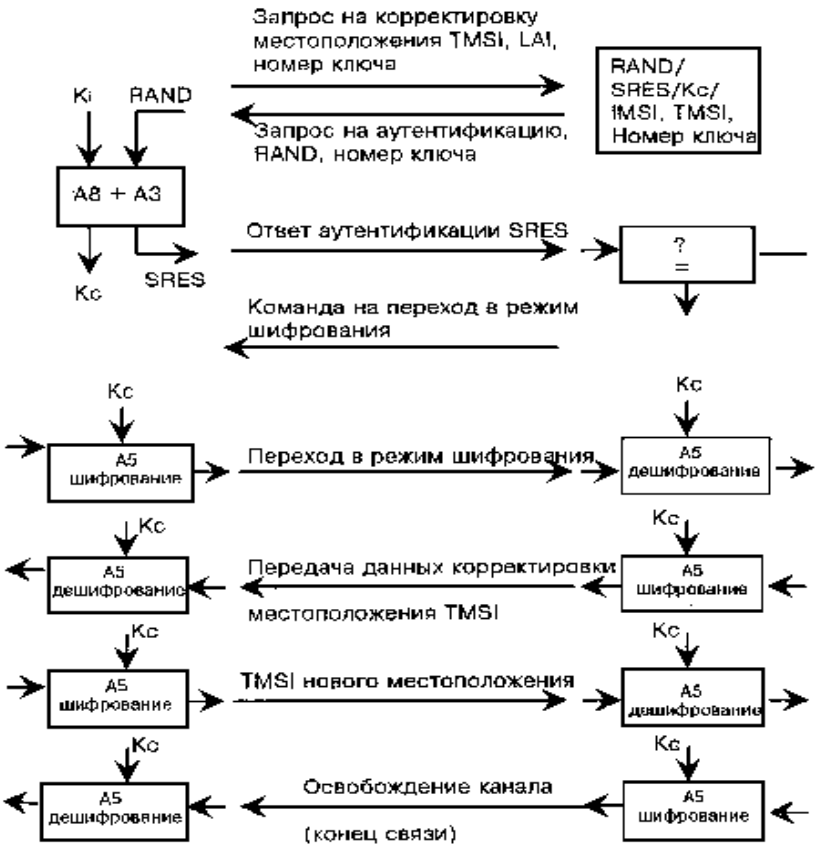
Конфиденциальность идентификационного номера означает, что оператор должен защищать телефонный номер, или номер IMSI, от неавторизованного доступа (либо от перехвата сообщений, передаваемых по радиоканалу)

Для этого каждому абоненту системы связи присваивается "временное удостоверение личности" - временный международный идентификационный номер пользователя (TMSI), который действителен только в пределах зоны расположения (LA). MSC посылает произвольный номер TMSI каждый раз во время установки связи, а при переходе из одной зоны в другую абоненту присваивается уже другой TMSI. Если абоненту еще не присвоен временный номер (например, при первом включении подвижной станции), идентификация проводится через международный идентификационный 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. Поэтому при смене абонентом местоположения также должна осуществляться безопасность передачи данных.

Обеспечение секретности в корректировке местоположения

Для того, чтобы выполнить процедуру корректировки местоположения, то по каналам управления осуществляется двухсторонний обмен служебными сообщениями между MS и BTS, содержащими временные номера абонентов TMSI. Для обеспечения секретности переименования TMSI, а также принадлежность номеров абоненту, в радиоканале необходимо обеспечить секретность передачи служебных сообщений.

На примере следующей схемы показано обеспечение секретности при перемещении абонента из одной зоны расположения в другую, и при этом абонент проводит сеанс связи.



1) MS вместе с временным номером TMSI, соответствующим прежней зоне расположения, уже зарегистрирована в регистре перемещения VLR
2) MS переходит в новую зону.
3) Происходит процедура опознавания, которая проводится по старому, зашифрованному в радиоканале TMSI, передаваемому одновременно с наименованием зоны расположения LAI
4) LAI дает информацию центру коммутации MSC и центру управления о направлении перемещения подвижной станции и позволяет запросить прежнюю зону расположения 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.

Общий состав секретной информации и ее распределение в аппаратных средствах GSM

Секретной считается следующая информация:
RAND, SRES, Ki, Kc, алгоритмы: A3, A8, A5; CKSN - номер ключевой последовательности шифрования, указывает на действительное число Kc, чтобы избежать использования разных ключей на передающей и приемной сторонах; TMSI.

В таблице приведены сведения распределения секретной информации в аппаратных средствах.

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

Литература

1) Материалы по информационным технологиям, предоставленные Кунегиным С.В. http://www.aboutphone.info/js/kunegin/gsm/4_5.html
2) Understanding Telecommunication. Security Function. http://www.ericsson.com/support/telecom/part-d/d-6-4.shtml
3) Мобильная безопасность (А Осадчук) http://users.g.com.ua/~batmanb/box/6/16.shtml
4) Мошенничество в сетях мобильной связи/сотовик http://www.sotovik.ru/news/articles/article_69.html