SIM-карта

Рассказ об устройстве, параметрах и функциональных возможностях SIM-карт сотовых телефонов стандарта GSM.

Самый распространенный микрокомпьютер

Удивить микрокомпьютером сегодня кого-нибудь уже непросто - они окружают людей повсеместно. И это уже не только разнообразные "наладонники" - PDA или калькуляторы, но и многочисленные микроконтроллеры средств автоматики, вовсю проникающие уже и в обычную бытовую технику. Но все эти устройства, выпускаемые большим числом фирм, имеют разную архитектуру и параметры. А вот наиболее распространенной моделью является изделие, большинство из пользователей которых даже и не подозревают, что это микрокомпьютер. Находится он в SIM-картах, используемых в сотовых телефонах стандарта GSM, а число владельцев таких телефонов на нашей планете уже приближается к миллиарду человек!

Возникновение SIM-карт

SIM-карты являются неотъемлемыми частями сотовых телефонов GSM, однако телефоны многих других стандартов вполне обходятся без них. Зачем же они потребовались?

Для того чтобы мобильный телефон мог обслуживаться в какой-либо сотовой сети, он должен быть для нее "своим" и иметь индивидуальное "имя", по которому сеть будет к нему обращаться. "Своим" в сотовой сети телефон становился путем "прописки" - регистрации его "имени" в абонентской базе системы. А вот в качестве "имен" телефонов, начиная с самых первых систем сотовой связи, служили специальные индексы, в качестве которых, обычно, использовались уникальные заводские номера аппаратов и их электронные аналоги - Electronic Serial Number (ESN). Именно этот номер мобильный телефон автоматически и сообщал сотовой сети при обращении к ней для выполнения звонка. Аналогично и вызов на телефон со стороны сети передавался по его ESN. Но вот здесь и возникли проблемы.

Все было предельно просто, когда, например, компания Ericsson создавала первую сотовую сеть стандарта NMT-450 в Саудовской Аравии. Она поставляла все оборудование - от коммутатора сотовой сети до мобильных телефонов, номера которых, естественно, могли задаваться в любой удобной форме и, кроме того, - были известны еще при производстве. Поэтому все операции по их "прописке" в сети могли быть выполнены даже прямо на заводе. Но дальше ситуация усложнилась. Число производителей сотовых телефонов стало непрерывно расти, и у всех из них использовались свои собственные буквенно-цифровые системы обозначения заводских номеров аппаратов. Такой разнобой исключал возможность их простой и единообразной записи в базе. Кроме этого, для предотвращения ошибок при регистрации номеров телефонов, целесообразно максимальное исключение из этого процесса людей, а также устранение всех видов помех, что лучше всего достигается при непосредственном подключении телефона к оборудованию сети. Другими словами, для "прописки" телефона его всегда надо было привозить к сотовому оператору. Честно говоря, проблема с различием в системах обозначений заводских номеров телефонов разных производителей для современного оборудования не очень существенна и при большом желании могла бы быть решена путем записи в телефоны каких-либо других номеров, обеспечивающих их однозначную регистрацию в абонентской базе сотовой сети. Но это не исключало необходимость непосредственного "контактирования" телефона с оборудованием сети при его прописке. Таким образом, при любой замене телефона абоненту обязательно надо было ехать с ним в отдел обслуживания сотовой компании.

Впервые задача устранения этого требования была поставлена в начале 90-х годов двадцатого века перед разработчиками только еще создававшегося тогда нового "общеевропейского" цифрового стандарта сотовой связи - GSM. Вот именно ими и было предложено разделить функции идентификации оборудования и абонентов.

Для идентификации телефонов в стандарте GSM используется специальный 15-значный уникальный номер Международного Идентификатора Мобильного Оборудования - International Mobile Equipment Identifier (IMEI), присваиваемый каждому аппарату при производстве (он также пишется на упаковочной коробке и на самом телефоне - под аккумулятором) и сообщаемый им сотовой сети при начале обмена.

Параметры же абонента были вынесены в специальный сменный модуль - Subscriber Identity Module (SIM), вставляемый в телефон.

По замыслу разработчиков стандарта GSM, код оборудования IMEI используется лишь для проверки "легальности" телефонов - сотовая сеть отказывает в обслуживании "незаконным" (например, украденным) аппаратам, чьи номера значатся в специальном "стоп листе" (если быть более точным, то существуют даже три списка - "черный", "серый" и "белый", но сути дела это не меняет). Так как обмен номерами всех "подозрительных" телефонов может производиться непосредственно между сотовыми сетями, то для разрешения обслуживания легальных телефонов нет необходимости в какой-либо их регистрации в сети, и абонент может самостоятельно менять телефоны по своему усмотрению. Кроме этого, надо отметить, что и сама проверка кода IMEI в сетях GSM не является обязательной и поддерживается далеко не всеми компаниями. Именно в результате этого обстоятельства в мире и существует подпольный рынок торговли ворованными телефонами GSM. Однако именно размах такой торговли привел к возникновению определенных сдвигов в данном направлении и, возможно, вскоре обмен кодами IMEI "потерянных" сотовых телефонов между сетями будет полностью отлажен, и проверки легальности телефонов станут выполняться повсеместно.

Ну а что касается SIM-карт, то они содержат все данные, необходимые для однозначной идентификации самого абонента. При этом SIM-карты могут программироваться заранее, а потом, продаваться в виде полностью готового товара в любой торговой точке. Купивший ее пользователь может самостоятельно, как вставить ее в свой сотовый телефон, так и переставить в любой другой. Во всех этих случаях его визит в сотовую компанию для проведения каких-либо технических манипуляций с телефоном или SIM-картой - совершенно не нужен.
Типы и возможности SIM-карт

В принципе, SIM-карта могла бы быть сделана предельно простой и содержать только идентификационный номер абонента. Но ее создатели пошли другим путем и сразу реализовали в ней функции, связанные не только с идентификацией абонента, но и с проверкой подлинности карты (аутентификацией) и шифрацией переговоров. Другими словами, весь комплект функций, выполняемых в других стандартах непосредственно телефоном, в GSM поделен между самим аппаратом и SIM-картой. Все чисто "связные" операции (прием и передача сигналов, их модуляция и детектирование, воспроизведение звуков и отображение символов на дисплее и т. п.) выполняются в телефоне, а все, что касается персональных данных - реализуется в SIM-карте. В результате такого подхода совершенно исправный телефон GSM самостоятельно (без SIM-карты) обеспечивает возможность выполнения только лишь звонков "SOS" (обычно по международному коду 112) в аварийные службы: полиция, пожарные, медицинская помощь и т. п. - это требование было изначально заложено в стандарт. С другой стороны, необходимость

выполнения в SIM-карте операций по обработке информации привела к реализации ее по принципу специализированного вычислителя, работающего под управлением своей операционной системы и содержащего все основные элементы микро-ЭВМ: 8-разрядный процессор, узлы ввода и вывода информации, а также постоянную (ROM), оперативную (RAM) и перепрограммируемую (EEPROM) память. Именно в энергонезависимой, но изменяемой памяти EEPROM (в современных SIM-картах она имеет емкость до 64 кбайт), и размещается вся прикладная информация - как пользовательская, так и служебная.

По своей вычислительной мощности SIM-карты вполне сопоставимы с первыми персональными компьютерами восьмидесятых годов прошлого века и достижения современной микроэлектроники позволяют постоянно увеличивать их возможности. В результате этого, в SIM-картах стали реализовываться и многие другие функции: записные книжки, емкостью до 100 и более телефонных номеров с именами, списки последних сделанных и принятых вызовов и т. п.

Поистине революционные изменения в любом телефоне, поддерживающем фазу развития стандарта GSM 2+ (сюда попадают практически все модели, выпуска после 1998 г.) совершает созданная несколько лет тому назад технология SIM Application Toolkit (STK). Она базируется на широком использовании для обмена информацией SMS-сообщений и представляет собой специальные программные приложения, записываемые на SIM-карте в виде наборов исполняемых процедур и команд. Под управлением таких программ телефон становится способен автоматически выполнять различные последовательности действий. Это может быть звонок по определенному номеру, отправка короткого сообщения по определенному номеру и с определенным содержанием, отправка электронной почты или факса и т. п. Все эти процедуры, естественно, могут выполняться и вручную, но автоматизация процесса существенно упрощает и ускоряет пользование такими услугами. В их число могут входить: доступ к информационно-справочным службам (прогноз погоды, курс обмена валют, последние новости, обстановка на дорогах и т. п.), управление подключением и отключением используемых услуг сотовой сети, доступ в Интернет, оплата различных услуг с мобильного телефона, игры и т. д.

С позиций пользователя, новая технология проявляется в том, что на дисплее телефона с установленной STK-картой, помимо стандартного для данного аппарата набора пунктов меню, появляется еще один пункт - SIM-меню (или SIM Service), содержащий перечень дополнительных возможностей. Их набор определяется оператором мобильной сети GSM и может изменяться (даже оперативно!) без необходимости замены телефона или SIM-карты. Процесс пользования такими услугами проходит приблизительно в следующем порядке. В зависимости от выбираемых абонентом видов дополнительного сервиса с помощью SIM-карты, поддерживающей технологию STK, автоматически формируются и отправляются соответствующие SMS-запросы. Вся необходимая информация о результатах проведенных операций возвращается на телефон абонента также в виде SMS. STK-карты, емкостью 32-64 кбит, например, оснащаются даже специальным SIM-браузером, обеспечивающим доступ в Интернет с мобильного телефона без необходимости устанавливать дорогостоящее диал-ап соединение. Информация при этом также передается посредством SMS, что позволяет просматривать не только WAP-страницы, но и не очень сложные страницы HTML. В нашей стране телефоны с STK-картами могут использоваться уже в ряде сотовых сетей ("Би Лайн", "МегаФон", "Мобильные ТелеСистемы", "Сибирские Сотовые Системы-900").

Другими словами, современная SIM-карта - это многофункциональное и высокотехнологичное устройство, но проблемы могут быть и с ней.
Надежность SIM-карт

Чисто технически, SIM-карты представляют собой адаптированную под нужды мобильной связи разновидность чиповых смарт-карт, параметры которых задаются группой международных стандартов ISO 7816. Подобные карты изначально ориентировались на использование в платежных системах и поэтому, еще на этапе разработки, особое внимание было уделено надежности их работы в самых разных условиях, достаточной механической прочности и высокой стойкости к электрическим напряжениям, магнитным полям и другим воздействиям. В связи с этим, SIM-карты редко выходят из строя, и если вдруг телефон отказывается работать с картой, то надо, прежде всего, выяснить, что же телефону "не нравится".

Причины здесь могут быть разные, и о них телефон всегда выдает соответствующее сообщение на дисплее. Так, например, если SIM-карта заблокирована специальным кодом персонального идентификатора абонента - Personal Identification Number - PIN (защищает телефон от несанкционированного использования посторонними людьми), то на экране телефона и появится сообщение типа "Введите PIN-код". При изготовлении данный код (4-8 знаков) для каждой SIM-карты устанавливается индивидуально и выдается пользователю вместе с картой (хотя иногда он задается производителями и одинаковым сразу для целых групп карт и при этом даже предельно простым: "0000"). PIN-код вводится прямо с клавиатуры телефона, при этом, если Вы ошиблись в наборе кода, то его можно повторить, но не более 3 раз. В случае если все 3 раза PIN-код был введен неправильно, SIM-карта переходит в состояние временной блокировки и теперь уже требует ввести 8-значный код персонального ключа разблокировки - Personal Unblocking Key (PUK), который также выдается пользователю при продаже карты. Вводить его надо внимательно, т. к. после десяти ошибочных попыток ввода PUK-кода SIM-карта блокируется полностью и требуется ее замена, о чем и появляется сообщение на экране телефона с рекомендацией обратиться к сотовому оператору. Если же снятие блокировок прошло успешно, то значение PIN-кода может быть в любой момент изменено самим пользователем. Ключ же PUK - напротив, изменению не подлежит. Кроме кодов PIN и PUK существует также аналогичная пара кодов PIN2 и PUK2 (тоже содержится в документации на SIM-карту, получаемую пользователем), служащих для управления доступом к некоторым функциям (запрет входящих и исходящих вызовов, обнуление счетчика длительности и стоимости разговоров и др.). Неправильно набранный три раза код PIN2 блокирует управление этими функциями и для их разблокировки требуется ввести PUK2-код. Коды PIN и PIN2, а также PUK и PUK2 не следует путать - они имеют разные значения и выполняют разные функции.

Совсем по другой причине при включении телефона может появиться надпись "Вставьте SIM-карту". Если ее в телефоне нет, то тут ясно, что надо делать, а вот если карта установлена, то такое сообщение означает, что телефон ее "не видит". Чаще всего причиной этого может быть тривиальный плохой контакт между картой и телефоном. Действия здесь могут быть следующими. Прежде всего, надо попробовать вынуть SIM-карту и поставить ее на место еще раз. Если после этого телефон не начал работать, то можно попытаться промыть контакты на SIM-карте и в разъеме телефона этиловым спиртом или специальной чистящей жидкостью и легонько протереть салфеткой из мягкой не ворсистой ткани. Применять какие-либо более "сильные" средства вроде чернильной резинки или наждачной бумаги не следует. Дело в том, что контакты на SIM-карте и в телефоне - позолочены, что исключает их окисление. Повреждение же этого тонкого золотого покрытия неминуемо приведет к последующему ухудшению контактов. Также не следует, и стараться прикладывать большие усилия к SIM-карте, пытаясь поплотнее прижать ее к контактам, т. к. в итоге можно повредить ее, ведь, по сути, она представляет собой бескорпусную микросхему на пластиковой или керамической

подложке. Если же сомнения в плотности соприкосновения контактов действительно имеются, то вполне удовлетворительный результат иногда может дать просто небольшой листок бумаги, сложенный в несколько раз и положенный сверху SIM-карты так, чтобы он поджимал ее при подсоединении аккумулятора.

Если все описанные действия не дали результатов, то остается попытаться проверить работу телефона с другой SIM-картой, а эту карту - с другим телефоном. Возможно, таким способом удастся выявить "виновного".

Однако известны и случаи "не совместимости" некоторых типов SIM-карт с отдельными моделями телефонов. При этом в других сочетаниях и карты и телефоны работают нормально. Причиной этого может быть некоторый (допустимый стандартом!) разброс параметров сигналов, которыми обмениваются телефон и карта в процессе совместной работы. Проявляться такой эффект может, например, только при определенных условиях: по мере разряда аккумулятора, в жару или на морозе и т. п. Другой причиной подобной проблемы может быть несоответствие рабочих напряжений. Все ранние версии SIM-карт были рассчитаны на рабочее напряжение (поступающее с телефона) величиной 5,5 В, а современные карты обычно работают с напряжением 3,3 В. Несоответствие рабочих напряжений не приводит к выходу из строя телефона или карты, но может быть причиной их неудовлетворительного взаимодействия.

С организационных и юридических позиций наиболее успешное решение этой технической проблемы возможно только в случае, если телефон приобретался вместе с SIM-картой. В этом случае можно говорить о неработоспособности комплекта. В других случаях - задача сложнее, так как каждое из устройств, в принципе, работает. Единственным выходом здесь может быть только проверка телефона прямо в процессе его приобретения с той картой, с которой его планируется использовать.

Особый вопрос составляют так называемые "лоченые" телефоны, в которых установлена блокировка SP lock (SIM-lock), разрешающая работу телефона только в конкретной сотовой сети. Ее целью является "привязывание" абонента, т. е. создание ситуации, при которой человек, купивший телефон у определенного оператора, не имел бы возможности перейти с этим телефоном в другую GSM сеть.

Технически данный метод защиты реализуется программно и может быть осуществлен различными способами, но суть его заключается в следующем. Оператор заказывает у производителя партию телефонов, на которые в процессе изготовления устанавливается специальная версия программного обеспечения, содержащая защиту на основе уникальной совокупности кодов оператора (NCC) и страны расположения сети (MCC). Так как эти же коды содержит и SIM-карта, то при каждом включении телефон сверяет эти коды. Если они совпали, то телефон работает нормально, если нет, - на экране появляется соответствующая надпись.

В случае необходимости данный вид защиты может быть снят путем ввода прямо с клавиатуры телефонов специальных кодов разблокирования SIM-lock, обычно поставляемых производителем вместе с партией телефонов. Другим способом отключения блокировки (т. к. никаких аппаратных изменений в телефоне для ее ввода не производилось) является замена программного обеспечения. Операция не очень сложная и вполне может быть выполнена и кустарными методами. Строго говоря, если вновь установленное программное обеспечение вполне корректно, то и телефон будет работать без ошибок. Если же это требование не соблюдено, то в работе телефона могут наблюдаться самые различные отклонения: периодически такой аппарат будет пытаться

снова зарегистрироваться в сети, будут блокироваться исходящие вызовы, окажутся недоступными некоторые разделы меню и т. п.

Особый вопрос составляет стойкость SIM-карт против взлома. Именно для противодействия подобным попыткам, вся служебная часть перепрограммируемой памяти SIM-карты, где хранится специальный международный идентификационный номер абонента мобильной связи (International Mobile Subscriber Identity - IMSI), его индивидуальный шифровальный ключ (Ki) и программа криптографического алгоритма (A3), построена так, что информация из нее доступна только внутреннему процессору SIM-карты и никаким способом не может быть считана извне. Благодаря таким мерам "взлом" SIM-карты возможен только методом прямого подбора необходимых номеров, что достижимо лишь в случаях, когда карта на длительное время попадает в руки злоумышленников. Но даже и против таких действий во всех новых картах имеется специальная защита, основанная на ограничении общего числа допустимых обращений к карте, после достижения которого она блокируется и перестает работать. Это число задается достаточно большим, чтобы не проявляться при нормальном использовании SIM-карты в телефоне в течение всего реального времени "жизни" этих изделий. Однако установленное ограничение существенно меньше числа обращений, обычно требующихся для подбора номеров при взломе карты. Другими словами, SIM-карта достаточно надежно защищает абонента от различных попыток незаконного пользования связью за его счет.

Однако изворотливость злоумышленников не знает пределов, и довольно оригинальный метод быстрого взлома SIM-карт тоже был найден. Предельно кратко его суть заключается в том, что при обращении к SIM-карте активность внутреннего процессора, а, следовательно, и ток, потребляемый им через соответствующие контакты карты от внешнего источника питания, оказываются различными в случаях, когда задаваемый код полностью не соответствует требуемому или частично совпадает с ним. Таким образом, контролируя ток, потребляемый SIM-картой в процессе работы, ее взлом методом подбора номеров оказывается возможным выполнить значительно быстрее.

Другими словами, общим советом всем владельцам SIM-карт может быть только рекомендация не давать их посторонним людям, например, вместе с телефоном при его ремонте, техническом обслуживании или во временное пользование.