Секреты умных карт

Архитектура SIM

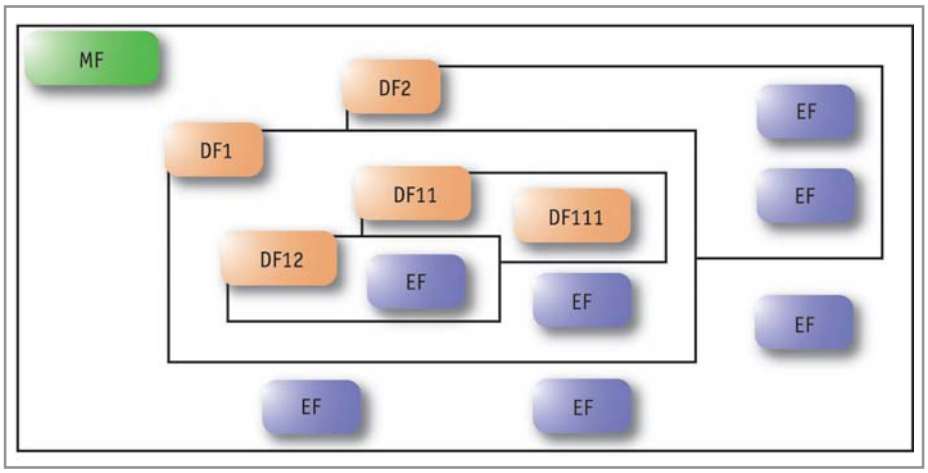
При покупке телефона, чтобы оживить новый аппарат и получить доступ в сеть, вы первым делом вставляете в него SIM-карту. Этот маленький кусочек меди, запаянный в пластик, на самом деле является сложным электронным мозгом мобильного устройства.

Смарт-карты (английское smart — умный, интеллектуальный) вполне оправдывают свое громкое название, хотя на первый взгляд и могут показаться достаточно простыми устройствами. Благодаря универсальности они нашли широкое применение не только в коммуникационных системах, но и в банковской сфере, медицине, транспорте, однако в данной статье мы ограничимся только областью сотовой связи. В мире мобильных коммуникаций смарт-карты принято называть SIM-картами (Subscriber Identity Module — устройство идентификации абонента).

Микрокомпьютер

Если вы хотите получить краткий ответ на вопрос, что же такое SIM-карта, то он будет следующим: это компьютер. И действительно, внутри SIM-карты размещены все устройства, которые мы привыкли видеть в персональных компьютерах: центральный процессор, оперативное запоминающее устройство, долговременная память, интерфейс ввода-вывода. Более того, в SIM-карту встроена настоящая операционная система, а в долговременной памяти крошечного чипа сформирована защищенная файловая система, где хранятся данные пользователя и разнообразные приложения, дополняющие и расширяющие функции устройства. В современных моделях SIM-карт также может содержаться java-машина, выполняющая приложения и тем самым обеспечивающая межплатформенную совместимость — точно так же, как это происходит, например, в мире персональных компьютеров.

Компьютер, размещенный в SIM-карте, представляет собой интегральную микросхему (микрочип). Часто присутствует и специальный блок, отвечающий »



▲ Организация файловой системы SIM-карты: MF — Master File (корневой каталог); DF — Dedicated File (директория); EF — Elementary File (файл)

▲ На дорогих моделях есть специальный механизм крепления SIM

» за выполнение функций защиты. В нем могут быть реализованы генерация случайного числа, блоки аппаратного шифрования информации, схемы, отслеживающие потенциальные попытки взлома карты (мониторинг питающего напряжения, тактовой частоты, температуры). Интеграция указанных устройств в единую микросхему препятствует проникновению злоумышленников к хранимой и обрабатываемой с помощью нее информации, поскольку подключиться к проводникам, соединяющим перечисленные устройства, в данном случае чрезвычайно сложно.

Структура памяти

Центральный процессор SIM-карты представляет собой восьмиразрядный микроконтроллер, как правило, основанный на одном из наиболее распространенных наборов команд — Intel 8051, Motorola 6805, Hitachi H8. Архитектура памяти имеет свои особенности. В общем случае присутствуют три типа памяти: постоянная (ROM — Read Only Memory), энергонезависимая (NVM — Non-Volatile Memory) и небольшой объем памяти с произвольным доступом (RAM — Random Access Memory). ROM объемом 10–90 кбайт используется для хранения операционной системы; NVM, типичный объем которой составляет 8–64 кбайт, хранит разнообразную секретную информацию, связанную с владельцем карты; RAM обычно используется для хранения временных переменных.

Объем RAM на SIM-карте невелик и составляет, как правило, всего от 256 байт до нескольких килобайт. Память NVM обладает рядом особенностей: быстродействие (3–10 мс на операцию записи), износостойкие ячейки памяти — производитель гарантирует около 100 000 циклов перезаписи. Это означает, что срок службы обычной смарт-карты ограничен — для SIM-карт он составляет приблизительно 3–5 лет.

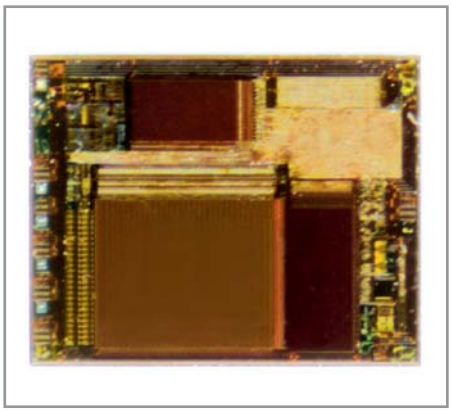
В последнее время все большее распространение получают чипы, в которых роль ROM выполняет NVM. Одним из главных преимуществ таких устройств является существенное сокращение сроков разработки специализированного программного обеспечения и запуска продукции в производство. Действительно, не нужно заказывать изготовление кристаллов по заранее подготовленной специальной маске. Вторая важная особенность новых чипов заключается в том, что сам производитель не разделяет на каком-либо этапе технологический маршрут для изготовления карт с различным содержимым ROM под нужды того или иного заказчика — для всех выпускается одинаковая продукция. В этих чипах объем памяти, отводимый для хранения операционной системы и данных, может быть сконфигурирован практически произвольно. После записи системы часть NVM-памяти может быть превращена в ROM путем установки специальных флагов, после чего перезапись этого участка NVM будет невозможна.

Файловая система

Не вдаваясь в физические и электрические параметры SIM-карты, сосредоточим наше внимание на особенностях организации записи данных. Файловая система SIM-карты построена по иерархической схеме, в рамках которой может присутствовать три типа файлов. Это так называемый мастер-файл (MF — Master File, его можно представить как своего рода корневую директорию), директории (DF — Dedicated File) и элементарные файлы (EF — Elementary File). Директории могут содержать элементарные файлы и другие поддиректории. Одна часть файлов может нести в себе административные данные, другая необходима для работы приложений, размещенных на карте; большинство же используется телефоном для, например, записной книжки или записи SMS.

Каждый из файлов содержит заголовок, где указан его тип, характеристики, условия доступа, уникальный идентификатор (FID) и другие параметры. Помимо заголовка у файла имеется тело, где записаны сохраненные данные. Естественно, что у директорий тела отсутствуют. Элементарные файлы подразделяются на три подтипа. Первый из них — это обычные бинарные файлы, два других подтипа — циклические и линейно-фиксированные — составляют файлы, содержимое тела которых логически разбито на записи. Для доступа к содержимому обычного бинарного файла достаточно выбрать сам файл. В случае с файлами, состоящими из записей, нужно в дополнении указать, к какой именно из них следует обращаться. Отличие циклического файла заключается в следующем: если выбрана последняя запись в файле, а поступила команда выбрать следующую, циклическом файле бу- »

▲ В центре платы расположен микрочип на кремниевом кристалле



▲ Увидеть архитектуру микрочипа можно при сильном увеличении

▲ Производителей SIM-карт не меньше, чем производителей телефонов

» дет выбрана первая запись. В линейно-фиксированном подобный выбор не допустим. Циклические файлы удобны для организации каких-либо счетчиков, линейно-фиксированные — для хранения SMS и записной книжки.

Файловая система SIM-карт имеет достаточно высокий уровень защиты. Прежде всего, это условия доступа для выполнения различных операций с файлами, такими, например, как чтение и запись. В заголовке у каждого из элементарных файлов указано, по какому условию становится возможной та или иная операция. Скажем, файл записной книжки можно прочесть только в том случае, если SIM-карте предъявлен код PIN1. Такое же условие распространяется и на запись. Некоторые файлы вообще никогда нельзя прочесть и/или записать, или, наоборот, чтение возможно всегда, даже когда ни один из кодов не предъявлен. Всего существует 16 различных уровней доступа. Слово «уровень» здесь можно взять в кавычки, поскольку нельзя однозначно сказать, что, предъявив более высокий «уровень», вы получаете доступ к низким «уровням» автоматически.

Коды доступа, такие, например, как PIN1 и PIN2, которые получает абонент, покупая подписку у своего оператора, передаются карте специальной командой, подаваемой с сотового телефона. Самый первый «уровень» — доступ разрешен всегда; затем идут доступ по PIN1 и PIN2, далее — доступ по административным кодам; наконец, самый старший — доступ запрещен всегда. Кроме этого, файлы могут быть помечены как непригодные к использованию — временно или навсегда. Это бывает крайне полезно при включении и отключении различных сервисов, предоставляемых картой, например GPRS.

Как сохранить данные?

Другая задача, решаемая в рамках файловой системы SIM-карты, заключается в сохранении целостности записываемой информации. Представьте себе знакомую ситуацию, когда внезапно пропадает питание, в то время как жесткий диск вашего компьютера перезаписывает содержимое какого-либо файла. Скорее всего, записываемая информация будет потеряна. Естественно, в случае с SIM-картой такая ситуация не до- »

Редактирование содержимого SIM-карты

Декарт, умеющий читать SIM-карты

Если вам необходимо прочесть и отредактировать данные, хранящиеся на SIM-карте, это можно сделать и с помощью мобильного телефона. Однако его возможности часто ограничены элементарным набором операций, да и пользоваться цифровой клавиатурой для редактирования текста крайне неудобно. В этом случае вы можете обратиться к специальным устройствам, предназначенным для чтения и редактирования SIM-карт, и соответствующему программному обеспечению, которое поставляется в комплекте с карт-ридерами.

Как правило, такие устройства можно приобрести у производителей самих SIM-карт. Например, компания Oberthur Card Systems выпускает несколько комплектов подобного оборудования. С помощью GemConnect MySIMeditor можно получить полную информацию о SIM-карте: IMSI (International Mobile Subscriber Identity); ICCID (SIM Card Serial Number); телефонный номер; имя сотового оператора; максимальное число и размеры возможных записей, адресную книгу, SMS. Вы сможете также управлять секретными кодами SIM-карты: осуществлять проверку, модификацию, разблокировку PIN1, PIN2. Однако цена этих оригинальных устройств достаточно высока (до $100), и на российском рынке их не так просто найти. Существует и дешевая альтернатива — карт-ридеры и соответствующее программное обеспечение, производимые сторонними разработчиками. Большой известностью пользуется продукция компании Dekart (www.dekart.com). Dekart SIM card reader, внешне напоминающий флеш-драйв, можно приобрести за $30, а программу Dekart SIM Manager 1.08 — всего за $10. Это простое в использовании и нетребовательное к системным ресурсам приложение работает с любыми SIM-картами. При загрузке содержимого карты в компьютер Dekart SIM Manager позволяет просматривать, редактировать, осуществлять поиск и сортировать записи в телефонной книге, управлять резервными копиями карты. Программа обладает средствами импорта и экспорта адресных книг. Так же как и GemConnect, Dekart SIM Manager может активировать и дезактивировать PIN-код карты.

» пустима в принципе. Ведь если, например, шел процесс обновления файла-ключа и в этот момент пропало питание, то уже никто не будет знать, какой именно ключ необходимо предъявлять — новый так и не был записан, а старый уже безвозвратно испорчен. Ситуация осложняется еще и тем, что у карты нет выключателя питания, как у компьютера, а пользователь может вынуть ее из телефона в самый неподходящий момент.

Для решения указанной проблемы используется специальный программный механизм, реализованный в рамках операционной системы. Основная его идея заключается в следующем: перед началом модификации данных заранее создается резервная копия той области памяти, в которой нужно провести изменения (в NVM-памяти), после чего выставляется специальный флаг (также в NVM-памяти), указывающий на то, что копия создана. Только после этого система приступает к самим изменениям. После окончания модификации данных флаг сбрасывается. На этапе, когда питание на карту подано, при запуске, операционная система проверяет этот флаг и, если он установлен, восстанавливает информацию. После восстановления флаг сбрасывается. Подобный алгоритм обеспечивает восстановление информации при возникновении сбоев в процессе изменения данных. Кроме того, для особо критичных файлов вычисляется контрольная сумма.

Ввод и вывод

Для общения с внешним миром посредством интерфейса ввода-вывода операционная система карты способна воспринимать различные команды. Условно

▲ С помощью MySIMeditor можно редактировать содержание SIM

▲ Карт-ридер компании Gemplus совместим с U(SIM)-картами

их можно разделить на ряд основных подгрупп: работа с файлами (выбор, чтение, изменение содержимого); работа с кодами доступа; административные команды; изменение флага пригодности к использованию того или иного файла; запуск алгоритма аутентификации. Команда представляет собой последовательность байт, передаваемых на карту. Первый байт называется классом, затем следует байт — идентификатор инструкции, далее три байта — параметры команды. После некоторых команд могут следовать данные. По завершении проверки и обработки карта передает два байта ответа, исходя из которых телефон определяет, все ли прошло успешно и нужно ли забрать какие-либо данные.

Своими руками?

Итак, мы убедились в том, что SIM-карта, используемая в мобильных аппаратах, представляет собой сложное интеллектуальное устройство, способное выполнять все те же операции, которые привычно ассоциируются с компьютерной сферой. Одним из основных стандартов для SIM-карт является выпущенный ETSI (European Telecommunications Standards Institute) документ, в котором описывается взаимодействие между устройством идентификации абонента и мобильным оборудованием в системах цифровой сотовой связи. Этот стандарт сокращенно называется GSM 11.11 — все спецификации находятся в свободном доступе, поэтому любой желающий может подробно узнать о физических и электрических параметрах SIM, а также назначении контактов интерфейса ввода-вывода, устройстве файловой системы и списке команд, ею воспринимаемых.

Обладая этими знаниями, можно самостоятельно сконструировать устройство для чтения SIM-карт или купить готовые модули (карт-ридер, программатор). Однако не стоит забывать, что нарушение конфиденциальности данных, записанных на не принадлежащих вам микрочипах, может повлечь за собой юридические последствия.

■ ■ ■ **Дмитрий Апраксин**