Открытым текстом

Безопасность в сетях GSM

Сотовый телефон стал привычным атрибутом многих людей самых различных профессий и слоев общества. Ну а для бизнесменов он, помимо всего прочего, является еще и рабочим инструментом, который должен уметь хранить секреты своего хозяина.

Действительно, что может быть проще, чем сделать важный звонок из кабины лимузина и провести переговоры о планируемых поставках товара? Разумеется, дело здесь не просто в удобстве, а в экономии времени, которое, как известно, для бизнесмена — деньги. Понятно, что пользу сотового телефона в этой сфере сложно переоценить. Но вот можно ли ему доверять важную информацию?

Сегодня существует немало различных стандартов сотовой связи. Наиболее распространенным из них является формат GSM. Поэтому в последнее время все более актуальными становятся вопросы, связанные с налаживанием механизмов безопасности, реализованных именно в этом стандарте. Как ни банально это прозвучит, но злоумышленники не дремлют — к сожалению, сегодня трудно кого-либо удивить прослушиванием разговоров, различными клонами и другими сотовыми мошенничествами. Мы попробуем разобраться, каким образом обеспечивается безопасность в сетях стандарта GSM, что входит в обязанности оператора, а что зависит от самого абонента.

Три кита безопасности GSM

Перед тем как вести разговор о механизмах безопасности, необходимо сказать несколько слов об архитектуре сети. Мы не »

» будем углубляться в подробности, а рассмотрим только два основных модуля — телефон и систему базовых станций. Обмен информацией между ними ведется по радиоканалу, так что возможность перехвата конфиденциальных данных у злоумышленников имеется. Кроме того, в телефоне выделяется еще один самостоятельный блок — SIM-карта.

В каждом из выделенных нами модулей реализованы собственные механизмы обеспечения безопасности. Так, SIM-карта отвечает за использование алгоритмов A3 и A8, а также содержит секретный код Ki и номер TMSI (в ходе дальнейшего изложения мы расшифруем смысл всех этих аббревиатур). Сам сотовый телефон поддерживает технологию A5 и хранит собственный уникальный номер IMEI. В программном же и аппаратном обеспечении системы базовых станций реализованы все перечисленные алгоритмы защиты, а в специальных базах данных хранятся все секретные коды.

Четыре цифры или отпечатки пальцев

В словаре термин «идентификация» расшифровывается как отождествление анализируемого объекта с одним из известных. В нашем случае SIM-карта пытается «узнать» человека, который хочет воспользоваться сотовым телефоном. Если она определит, что это ее хозяин, то доступ ко всем функциям ему будет открыт, в противном же случае мобильный телефон окажется попросту недоступным для использования (разумеется, звонок экстренного вызова можно сделать даже без SIM-карты). Идентификация предназначена для защиты владельца сотового телефона от несанкционированного использования его SIM-карты, а следовательно, и денег, лежащих на его счету у оператора.

В сетях сотовой связи обычно используется парольная идентификация. То есть человек подтверждает свою личность персональным паролем. В сети GSM он носит название PIN-кода (PIN — Personal Identification Number — личный идентификационный номер) и является произвольной комбинацией, состоящей из четырех цифр, как и у кредитной карты. Первоначально PIN-код выдается оператором сотовой связи вместе с SIM-

▲ Для радиоперехвата можно использовать приемники AR8600

▲ Код IMEI вы можете найти под аккумулятором своего телефона

картой, но в будущем он может быть изменен (и лучше это сделать сразу же после покупки) владельцем телефона. Сам по себе пароль из четырех цифр не считается серьезной защитой, ведь подобрать его можно очень быстро. Для того чтобы избежать этого, существует ограничение в три попытки ввода PIN-кода. Если человек так и не смог сделать это правильно, SIM-карта блокируется.

Для разблокировки SIM-карты используется PUK-код (PUK — Personal Unlock Key — личный код разблокирования). Он также выдается оператором сотовой связи вместе с SIM-картой, но уже не может быть изменен владельцем телефона самостоятельно. Кстати, число попыток правильного ввода PUK-кода также ограничено. После десятого неправильного ввода числа SIM-карта заблокируется полностью, после чего ее придется восстанавливать в сервисном центре оператора сотовой связи.

В целом механизм идентификации в сетях сотовой связи формата GSM достаточно надежен. Вот только вводить PIN-код каждый раз, когда нужно использовать телефон, уж очень неудобно. Так что в реальной жизни идентификация запускается только при включении аппарата. Это, конечно же, сильно снижает надежность защиты, зато делает использование телефона гораздо более удобным.

Вообще, увеличение удобства использования за счет снижения надежности в компьютерной и коммуникационной сферах используется достаточно часто. Однако все увеличивающееся число краж сотовых телефонов заставляет специалистов искать новые способы идентификации. Наиболее перспективным решением в этой области выглядит использование биометрических технологий, в частности сканирования отпечатков пальцев. Такие сотовые телефоны появились в прошлом году. Однако выпускаются они небольшими сериями и стоят дорого, к тому же сама технология еще не доработана и непривычна для рядовых пользователей. Впрочем, в последнее время наблюдается существенное снижение цен на полупроводниковые сенсоры отпечатков пальцев, а это значит, что уже в ближайшем будущем могут появиться телефоны с возможностью биометрической идентификации и стоимостью лишь на $10–15 дороже аналогов без сканеров.

Атака клонов

Следующим механизмом безопасности является аутентификация — подтверждение прав на проведение тех или иных операций. В данном случае подтверждается право SIM-карты работать в сети сотовой связи GSM. Аутентификация производится по специальному алгоритму A3. Он является закрытым, то есть секретным: подробности его работы известны только разработчикам, производителям сотового оборудования и операторам. По крайней мере, так должно было быть, однако на самом деле алгоритм A3 не является особо большим секретом и знаком многим профессиональным мошенникам. Впрочем, это нисколько не облегчает их жизнь. Дело в том, что в основе алгоритма лежат односторонние операции, а это значит, что по результату его работы невозможно восстановить исходные данные.

В общих чертах процесс аутентификации выглядит следующим образом. Сотовый телефон отправляет на базовую станцию сети запрос на подключение. В ответ ему передается случайно сгенерированная последовательность цифр (RAND/RND — от английского random — произвольный, случайный, выбранный наугад). Используя эти данные и свой собственный секретный ключ Ki, SIM-карта преобразовы- »

▲ На современные бизнес-модели телефонов (Pantech GI100) и КПК (HP iPAQ hx2700) ставятся сканеры отпечатков пальцев

» вает их по алгоритму A3, получая в итоге значение SRES (Signed RESult — подписанный результат). В то же время базовая станция производит подобные вычисления, выбирая подходящий Ki из своей базы данных. Получив SRES от сотового телефона, она сравнивает его с результатом, полученным по итогам собственных вычислений. Если оба числа совпадают, SIM-карта проходит аутентификацию, то есть мобильное устройство получает право работать в данной сети сотовой связи.

Из принципа работы механизма аутентификации видно, что секретные данные (в частности, Ki) никогда не передаются в радиоэфир, то есть их невозможно перехватить. Это должно гарантировать надежность аутентификации и исключить реализацию поддельной процедуры злоумышленником. По крайней мере, так должно было быть в теории. К сожалению, сегодня алгоритм A3, бывший некогда весьма надежной защитой, уже устарел. Следствием этого стало повсеместно появление клонов сотовых телефонов. Хотя, если быть точным, речь идет о клонах SIM-карт, но это словосочетание как-то не прижилось.

Суть данного вида мошенничества заключается в следующем: злоумышленник получает в руки SIM-карту, затем с помощью специального оборудования подключает ее к компьютеру и за несколько часов работы специализированного ПО узнает значение Ki. Это позволяет ему перепрограммировать другую SIM-карту так, чтобы она проходила аутентификацию от имени жертвы.

Раньше оборудование для реализации такой операции стоило очень дорого, да и времени на расшифровку секретных данных нужно было немало. Сегодня же купить комплект клонирования можно за $200, а с задачей по получению Ki любой современный ПК справится всего за несколько часов. Таким образом, проблема копирования стоит сегодня очень остро. Для того чтобы защититься от этой напасти, никогда и никому нельзя отдавать свою SIM-карту.

Меня зовут никто

Для многих людей большое значение имеет поддержка анонимности во время разговора по сотовому телефону. Под анонимностью подразумевается невозможность определения абонента путем перехвата радиосигнала, излучаемого его аппаратом или базовой станцией. Для обеспечения механизма анонимности при первом включении телефона с новой SIM-картой ей присваивается TMSI (Temporary Mobile Subscriber Identify) — временный идентификатор мобильного абонента. При этом в базе данных делается запись, которая приводит в соответствие TMSI определенному телефонному номеру. Эта процедура повторяется каждый раз при смене абонентом зоны сотовой сети.

В будущем при совершении всех звонков по радиоканалу передается не номер мобильного телефона, а TMSI. Таким образом, злоумышленник, даже перехватив сигнал, не может определить, для кого из абонентов он предназначен. Конечно, мошенник может попытаться получить доступ к специальной базе данных, устанавливающей соответствие между TMSI и телефонными номерами. Однако каждый оператор сотовой связи достаточно надежно защищает всю конфиденциальную информацию. Кроме того, злоумышленник может получить нужные ему данные прямо с мобильного устройства путем перехвата излучаемого сигнала. Правда, для этого необходимо иметь прямой доступ к телефону и нельзя забывать, что TMSI меняется на совершенно иной во время перехода абонента в другую зону. Это является дополнительной защитой анонимности.

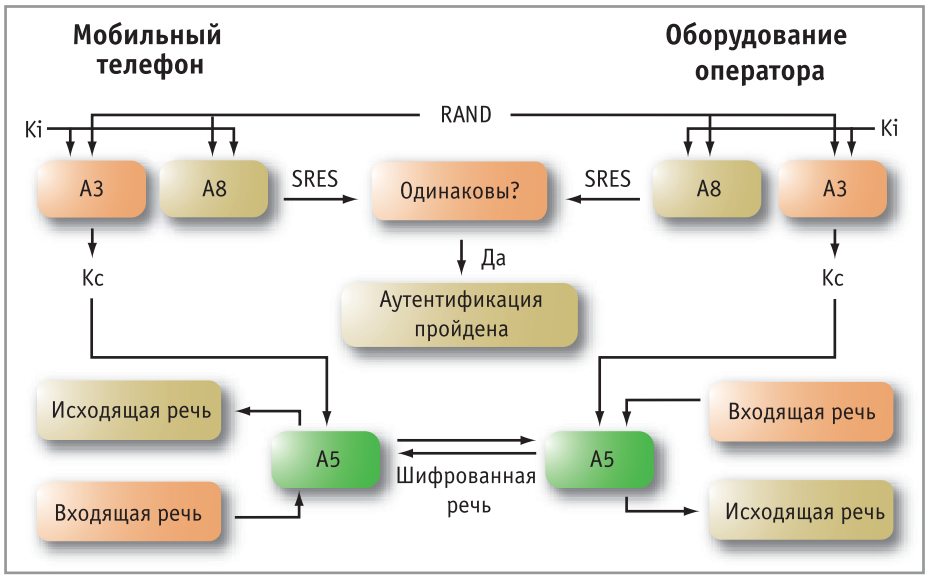
Экспорт запрещен

Еще одной достаточно серьезной опасностью использования сетей GSM, как, впрочем, и любого другого стандарта сотовой связи, является возможность перехвата радиосигнала. Сделать это, в общем-то, совсем не сложно. Для этого даже не нужно никакого специального оборудования, вполне можно обойтись устройствами, собранными обычными радиолюбителями. Более того, многие старые советские радиоприемники способны принимать сигналы с частотой, использующейся сегодня для сотовой связи. В аналоговых стандартах защита речи вообще не была предусмотрена. Это значит, что любой человек с помощью простейшего оборудования мог слушать все разговоры, ведущиеся в пределах доступа его приемника.

Естественно, такая ситуация никого не устраивала. Поэтому в стандарте GSM, который является цифровым форматом, предусмотрена возможность шифрования передаваемой речи. Для этого используется специальный криптоалгоритм. Речь идет о технологии A5, разработанной еще в прошлом веке — в 1987 году. Она реализует поточное шифрование на основе трех линейных регистров сдвига с неравномерным движением. A5 — закрытый алгоритм. Это значит, что принцип его действия известен только определенному кругу »

» лиц — разработчикам и производителям сотового оборудования, исследовательским центрам и т. д.

Алгоритм A5 был разработан Европейским институтом телекоммуникационных стандартов (ETSI — European Telecommunications Standards Institute). В его создании активное участие приняли спецслужбы стран НАТО, особенно Великобритании и Франции. Экспорт этой технологии во многие страны был строго ограничен. Для того чтобы обеспечить функционирование сотовых сетей стандарта GSM в других государствах, была разработана облегченная версия криптоалгоритма, получившая название A5/2. Впрочем, сегодня все эти запреты остались позади — в эпохе холодной войны. В современной России, как и в подавляющем большинстве государств, операторы GSM-сетей для защиты разговоров от прослушивания уже давно используют именно A5/1.



▲ Из схемы работы механизма аутентификации видно, что секретные данные никогда не передаются в радиоэфир

Защита информации не бывает дешевой

Но действительно ли так надежно предлагаемое нам шифрование? Сегодня известно, что в алгоритме A5 используются регистры 19, 22 и 23 бита. Сложив эти значения, мы получим 64-битный сеансовый ключ. К сожалению, приходится признать, что на данный момент даже такой защиты оказывается недостаточно. Она может быть взломана с помощью распределенной вычислительной системы за обозримый отрезок времени.

Более надежный алгоритм шифрования речи в сетях сотовой связи стандарта GSM был разработан в 2002 году совместными усилиями комитета по безопасности Ассоциации GSM, организации 3GPP (3rd Generation Partnership Project) и Комитета по алгоритмам безопасности Европейского института телекоммуникационных стандартов. Он получил название A5/3, однако его развитие и распространение оказалось весьма затруднено. Проблема заключается в том, что для ввода в эксплуатацию этой технологии оператор сети должен заменить не только программное обеспечение, но и часть дорогостоящего оборудования.

Открытым текстом

С шифрованием речи в сетях GSM связана и еще одна проблема. Дело в том, что оператор сотовой связи может вообще выключить эту возможность. В этом случае все разговоры будут передаваться в радиоэфир открытым текстом. Согласно сложившейся практике, шифрование в сетях сотовой связи может быть выключено по требованию спецслужб.

К сожалению, отключенное в благих целях шифрование речи может стать серьезной угрозой для всех владельцев мобильных телефонов. И действительно, операторы в подавляющем большинстве случаев не ставят своих клиентов в известность о предстоящем отключении шифрования. А это значит, что человек не может точно знать, защищен ли его разговор от прослушивания в данный отрезок времени. Правда, на экранах некоторых современных телефонов есть специальные символы, которые загораются во время отключения защиты, но многие ли абоненты обращают на это внимание? Так что приходиться признать, что сотовые сети стандарта GSM до сих пор довольно слабо защищены от прослушивания разговоров, причем не по вине абонентов. ■ ■ ■ **Марат Давлетханов**

Идентификация сотового телефона

Проскрипционные списки

IMEI (International Mobile Equipment Identity) — это международный идентификатор мобильного устройства. Этот код хранится в памяти самого аппарата и не может быть изменен стандартными средствами. Разработчики стандарта GSM предполагали, что с его помощью им удастся предотвратить воровство сотовых телефонов.

Мобильное устройство может сообщать базовой станции свой IMEI по специальному запросу, полученному с ее стороны. По логике вещей эта процедура должна осуществляться каждый раз при регистрации любого телефона в сотовой сети. При этом полученный от него IMEI ищется в трех списках: белом, сером и черном. В первом хранятся все «законопослушные» телефоны, во втором — подозрительные номера, за которыми необходимо наблюдение, в третьем — ворованные устройства. В зависимости от того, в каком из этих списков находится данный IMEI, выносится вердикт о разрешении работы в сети.

К сожалению, сегодня весь этот механизм не работает. Почему? Все дело в организационных вопросах. Согласитесь, нелегко обеспечить поддержку единой базы данных для сотен операторов по всему миру и реализовать нормальный доступ к ней или хотя бы регулярное обновление информации. Кстати, подобные черные списки ворованных ноутбуков есть у IBM, Toshiba и других крупных производителей компьютерной техники, однако, как и в случае с IMEI, эти меры не помогают бороться с воровством в глобальном масштабе.