**Краткий курс “Охраны безопасности жизнедеятельности” для владельца сотового телефона**

Так уж устроен мир, что любое техническое изобретение человеческого разума, расширяющее наши возможности и создающее для нас дополнительный комфорт, неизбежно содержит в себе и отрицательные стороны, которые могут представлять потенциальную опасность для пользователя. Не являются исключением в этом плане и современные средства мобильной связи. Дав нам относительную свободу, эти “чудеса техники” развязали руки и для многочисленной армии мошенников самого разного уровня. СОТА1 уже затрагивала тему “мобильной” безопасности. Обратимся к ней еще разок: повторенье – мать учения.

**Повторение пройденного**

Чтобы лучше понять проблемы, связанные с использованием мобильных телефонов, давайте вспомним, что они из себя представляют и как работают.

Мобильные телефоны сотовой связи фактически являются сложной миниатюрной приемо-передающей радиостанцией. Каждому сотовому телефонному аппарату присваивается свой электронный серийный номер (ESN), который кодируется в микрочипе телефона при его изготовлении и сообщается изготовителями аппаратуры специалистам, осуществляющим его обслуживание. Кроме того, некоторые изготовители указывают этот номер в руководстве для пользователя. При подключении аппарата к сотовой сети в микрочип телефона заносится еще и мобильный идентификационный номер (MIN). Мобильный сотовый телефон имеет большую, а иногда и неограниченную дальность действия, которую обеспечивает сотовая структура зон связи.

Вся территория, обслуживаемая сотовой системой связи, разделена на отдельные прилегающие друг к другу зоны связи или “соты”. Телефонный обмен в каждой такой зоне управляется базовой станцией, способной принимать и передавать сигналы на большом количестве радиочастот. Периодически (с интервалом 30-60 минут) базовая станция излучает служебный сигнал. Приняв его, мобильный телефон автоматически добавляет к нему свои MIN- и ESN-номера и передает получившуюся кодовую комбинацию на базовую станцию. В результате этого осуществляется идентификация конкретного сотового телефона, номера счета его владельца и привязка аппарата к определенной зоне, в которой он находится в данный момент времени.

Когда пользователь звонит по своему телефону, базовая станция выделяет ему одну из свободных частот той зоны, в которой он находится, вносит соответствующие изменения в его счет и передает его вызов по назначению. Если мобильный пользователь во время разговора перемещается из одной зоны связи в другую, базовая станция покидаемой зоны автоматически переводит сигнал на свободную частоту новой зоны.

**Тотальный шпионаж**

В настоящее время электронный перехват разговоров, ведущихся по сотовому телефону, стал широко распространенным явлением. Так, например, в Канаде, по статистическим данным, от 20 до 80 процентов радиообмена, ведущегося с помощью сотовых телефонов, случайно или преднамеренно прослушивается посторонними лицами.

Электронный перехват сотовой связи не только легко осуществить, он, к тому же, не требует больших затрат на аппаратуру, и его почти невозможно обнаружить. На Западе прослушивание и/или запись разговоров, ведущихся с помощью беспроводных средств связи, практикуют правоохранительные органы, частные детективы, промышленные шпионы, представители прессы, телефонные компании, компьютерные хакеры и т.п.

В западных странах уже давно известно, что мобильные сотовые телефоны, особенно аналоговые, являются самыми уязвимыми с точки зрения защиты передаваемой информации. Принцип передачи информации такими устройствами основан на излучении в эфир радиосигнала, поэтому любой человек, настроив соответствующее радиоприемное устройство на ту же частоту, может услышать каждое ваше слово. Для этого даже не нужно иметь особо сложной аппаратуры. Разговор, ведущийся с сотового телефона, может быть прослушан с помощью продающихся на Западе программируемых сканеров с полосой приема 30 кГц, способных осуществлять поиск в диапазоне 860-890 МГц. Для этой же цели можно использовать и обычные сканнеры после их небольшой модификации (которая, кстати, весьма подробно описана в Интернете). Перехватить разговор можно даже путем медленной перестройки УКВ-тюнера в телевизорах старых моделей в верхней полосе телевизионных каналов (от 67 до 69), а иногда и с помощью обычного радиотюнера. Наконец, такой перехват можно осуществить с помощью ПК.

Более совершенны с точки зрения защиты информации цифровые сотовые телефоны, передающие информацию в виде цифрового кода. Однако, используемый в них алгоритм шифрования Cellular Message Encryption Algorithm (CMEA) может быть вскрыт опытным специалистом в течение нескольких минут с помощью персонального компьютера. Что касается цифровых кодов, набираемых на клавиатуре цифрового сотового телефона (телефонные номера, номера кредитных карточек или персональные идентификационные номера PIN), то они могут быть легко перехвачены с помощью того же цифрового сканера.

Следует отметить, что такие часто рекламируемые возможности беспроводного телефона, как “цифровой код безопасности” (digital security code) и “снижение уровня помех” (interference reduction), нисколько не предотвращают возможность перехвата разговоров. Они только препятствуют несанкционированному использованию этого телефона.

**“Незаконнорожденные” телефоны**

Мошенничество в сотовых системах связи, известное еще под названием “клонирование”, основано на том, что абонент использует чужой идентификационный номер (а, следовательно, и счет) в корыстных интересах. В связи с развитием быстродействующих цифровых сотовых технологий, способы мошенничества становятся все более изощренными, но общая схема их такова: мошенники перехватывают с помощью сканеров идентифицирующий сигнал чужого телефона, которым он отвечает на запрос базовой станции, 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. (Об этом довольно подробно СОТА1 писала в статье от 23.11.2000г.)

Кража номеров осуществляется, как правило, в деловых районах и в местах скопления большого количества людей: шоссе, дорожные пробки, парки, аэропорты, - с помощью очень легкого, малогабаритного, автоматического оборудования. Выбрав удобное место и включив свою аппаратуру, мошенник может за короткий промежуток времени наполнить память своего устройства большим количеством номеров.

Наиболее опасным устройством является так называемый сотовый кэш-бокс, представляющий собой комбинацию сканера, компьютера и сотового телефона. Он легко выявляет и запоминает номера MIN и ESN и автоматически перепрограммирует себя на них. Использовав пару MIN/ESN один раз, он стирает ее из памяти и выбирает другую. Такой аппарат делает выявление мошенничества практически невозможным. Несмотря на то, что эта аппаратура на Западе пока еще редка и дорога, она уже существует и представляет растущую опасность для пользователей сотовой связи.

**Высоко сижу – далеко гляжу**

Оставим в стороне такую очевидную возможность, как выявление адреса абонента сотовой системы связи через компанию, предоставляющую ему эти услуги. Немногие знают, что наличие мобильного сотового телефона позволяет определить как текущее местоположение его владельца, так и проследить его перемещения в прошлом. Более того, в Росси такая слежка в скором времени может быть официально узаконена (в июле прошлого года Министерство связи РФ издало приказ, согласно которому операторы связи были обязаны собственными силами и за собственный счет подключать специальное оборудование для прослушивания телефонных разговоров и чтения сообщений электронной почты своих клиентов. И, хотя он был признан “частично недействительным”, разговоры об этом законопроекте не утихают – загляните на www.libertarium.ru – найдете кучу публикаций по теме СОРМ).

Текущее положение может выявляться двумя способами. Первым из них является обычный метод триангуляции (пеленгования), определяющий направление на работающий передатчик из нескольких (обычно трех) точек и дающий засечку местоположения источника радиосигналов. Необходимая для этого аппаратура хорошо разработана, обладает высокой точностью и вполне доступна.

Второй метод - через компьютер предоставляющей связь компании, который постоянно регистрирует, где находится тот или иной абонент в данный момент времени даже в том случае, когда он не ведет никаких разговоров (по идентифицирующим служебным сигналам, автоматически передаваемым телефоном на базовую станцию). Точность определения местонахождения абонента в этом случае зависит от целого ряда факторов: топографии местности, наличия помех и переотражений от зданий, положения базовых станций, количества работающих в настоящий момент телефонов в данной соте. Большое значение имеет и размер соты, в которой находится абонент, поэтому точность определения его положения в городе гораздо выше, чем в сельской местности (размер соты в городе составляет около 1 кв.км против 50-70 кв.км на открытой местности) и, по имеющимся данным, составляет несколько сот метров.

Наконец, анализ данных о сеансах связи абонента с различными базовыми станциями (через какую и на какую базовую станцию передавался вызов, дата вызова и т.п.) позволяет восстановить все перемещения абонента в прошлом. Такие данные автоматически регистрируются в компьютерах компаний, предоставляющих услуги сотовой связи, поскольку оплата этих услуг основана на длительности использования системы связи. В зависимости от фирмы, услугами которой пользуется абонент, эти данные могут храниться от 60 дней до 7 лет.

Такой метод восстановления картины перемещений абонента очень широко применяется полицией многих западных стран при расследованиях, поскольку дает возможность восстановить с точностью до минут, где был подозреваемый, с кем встречался (если у второго тоже был сотовый телефон), где и как долго происходила встреча или был ли подозреваемый поблизости от места преступления в момент его совершения.

**“Доступный” WAP**

Не меньше тревог возникает и у владельцев сотовых телефонов с поддержкой WAP. Как грибы после дождя появляются новые WAP-сайты, в том числе и российские, WAP-телефоны дешевеют и становятся доступны рядовым потребителям, операторы снижают тарифы на услуги передачи данных и вводят в эксплуатацию различные информационно-финансовые WAP-услуги, в том и числе и системы мобильной коммерции (m-commerce). Однако, чем больше сотовый телефон становится похож на мини-компьютер, тем больше вероятность доступа к конфиденциальной информации посторонних лиц.

Как в любой другой системе электронных платежей и обмена конфиденциальной информацией, вопрос безопасности транзакций – ключевое звено всей системы. Система мобильного интернета состоит из двух транспортных частей передачи информации – радиоканала сотовой связи и самой инфраструктуры интернета. В сетях GSM используются средства защиты протокола WAP, а в интернете - протокола TCP/IP. Но в этой, на первой взгляд неплохо защищенной, системе присутствует недоработка в точке сопряжения мобильной инфраструктуры и интернета. При перекодировке данных они остаются на какое-то время абсолютно незащищенными. Преобразования WTLS - SSL - WTLS осуществляются на WAP-шлюзе, и как раз в это время данные остаются незашифрованными и потенциально уязвимыми. Фактически это означает возможность постороннего вмешательства в передаваемую и принимаемую информацию, будь то e-mail, секретный пароль или обычные wml-страницы.

**Следи за собой. Будь осторожен.**

Проблема безопасности при использовании современных беспроводных средств связи достаточно серьезна, но, используя здравый смысл и известные приемы противодействия, ее можно, в той или иной степени, решить. Не будем затрагивать тех мер, которые могут предпринять только провайдеры связи (например, введение цифровых систем). Поговорим о том, что можете сделать вы сами.

Для предотвращения перехвата информации:

используйте общепринятые меры по предупреждению раскрытия информации: избегайте или сведите к минимуму передачу конфиденциальной информации, такой как номера кредитных карточек, финансовые вопросы, пароли. Прибегайте в этих целях к более надежным проводным телефонам, убедившись, однако, что ваш собеседник не использует в этот момент радиотелефон. Не используйте сотовые или беспроводные телефоны для ведения деловых разговоров;

помните, что труднее перехватить разговор, который ведется с движущегося автомобиля, т.к. расстояние между ним и перехватывающей аппаратурой (если та находится не в автомобиле) увеличивается и сигнал ослабевает. Кроме того, при этом ваш сигнал переводится с одной базовой станции на другую с одновременной сменой рабочей частоты, что не позволяет перехватить весь разговор целиком, поскольку для нахождения этой новой частоты требуется время;

используйте системы связи, в которых данные передаются с большой скоростью при частой автоматической смене частот в течение разговора;

используйте, при возможности, цифровые сотовые телефоны;

отключите полностью свой сотовый телефон, если не хотите, чтобы ваше местоположение стало кому-то известно.

Для предотвращения мошенничества:

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;

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. Этот способ самый легкий и дешевый, но следует помнить, что для опытного специалиста достаточно одного вашего выхода на связь, чтобы выявить MIN/ESN номера вашего аппарата;

регулярно меняйте через компанию, предоставляющую вам услуги сотовой связи, MIN-номер вашего аппарата. Этот способ несколько сложнее предыдущего и требует времени;

попросите компанию, предоставляющую вам услуги сотовой связи, установить для вашего телефона дополнительный 4-х значный PIN-код, набираемый перед разговором. Этот код затрудняет деятельность мошенников, так как они обычно перехватывают только MIN и ESN номера, но, к сожалению, небольшая модификация аппаратуры перехвата позволяет выявить и его;

наиболее эффективным методом противодействия является шифрование MIN/ESN номера (вместе с голосовым сигналом) по случайному закону. Но этот метод дорог и пока малодоступен.