плотностью населения, в основном сельского, наглядно демонстрирует более высокую техническую и экономическую эффективность этого стандарта по сравнению с UMTS.

Компания "ITC" является оператором сотовой сети стандарта IS-95 "CDMA Украина". Услуги предоставляются абонентам в гг. Киев и Чернигов, включая пригород в радиусе 50 км от города. Сеть построена на оборудовании производства "Lucent Technologies". Абонентам предоставляется качественная голосовая связь и услуга передачи данных со скоростью 14.4 Кбит/с практически по тарифам Укртелекома. Спрос на услугу передачи данных очень велик – до 50 % абонентов. В ближайшие несколько месяцев оператор планирует начать предоставлять в сети услуги первой фазы третьего поколения, скорость передачи данных будет достигать 153,6 кбит/с. Радиус действия базовой станции превысит 100 км, что позволит с помощью ретрансляторов обеспечивать связью значительные по площади районы сельской местности. Кроме Киева и Чернигова сети этого стандарта компания "ITC" планирует развернуть в Киевской области, Винницком и Житомирском регионах.

Кодовое разделение каналов, основанное на шумоподобных сигналах, изначально использовалось в системах связи военного назначения как средство защиты от помех и прослушивания, и реализованное в стандартах сотовой связи IS-95 и CDMA-2000 1X, в значительной степени отвечает требованиям по безопасности связи в проектируемой Национальной системе конфиденциальной связи Украины, поскольку в таких сетях связи предусмотрены меры по защите от несанкционированного доступа (аутентификация) и снижению возможности перехвата голосовой информации и данных.

Процедура аутентификации в сети "CDMA Украина" выполняется на основе ключа (A-key) и активизируется в исполнительном сотовом процессоре (ECP) при первоначальном внесении абонентского терминала в базу данных. На основе этого ключа, индивидуальных данных об абонентском терминале и случайного 56-битного числа, генерируемого ECP, а также криптографического алгоритма CAVE выполняется процедура аутентификации. Результатом работы алгоритма CAVE является особое 128-битное число, называемое SSD, которое хранится в ECP и абонентском терминале и используется в дальнейшем при выполнении процедур безопасности связи.

В стандарте CDMA предусмотрена реализация режима шифрования речи (Voice Privacy) и кодирования служебных сообщений. Для этой цели используется число SSD-B длиной 64-бита.

При работе в режиме шифрования речи на основе SSD-B при помощи криптографического алгоритма CAVE формируется случайное число VPMASK, различное для каждого сеанса связи. На основе VPMASK создается "индивидуальная маска длинного кода" (PLCM), имеющая длину ПСП, равную $2^{42} – 1$ бит, которая используется при формировании шумоподобного сигнала от абонентского терминала.

Вывод: Сети сотовой связи стандарта CDMA-2000 1X, которые могут быть развернуты в диапазонах 450, 700, 800, 1900, 2100 МГц, являются наиболее перспективной технологией для Национальной системы конфиденциальной связи Украины, поскольку по своим технико-экономическим показателям значительно превосходят другие системы 3G. На основе технологии CDMA-2000 1X в течение 2–3 лет могут быть развернуты защищенные от прослушивания и несанкционированного доступа региональные сети конфиденциальной связи, охватывающие всю территорию Украины, поддерживающие режимы высокоскоростной передачи данных, многосторонней конференции и оперативной связи.

Литература: ***1.*** *Третье поколение систем мобильной связи. Тезисы докладов. Международный научно-практический семинар IMT-2002, 10–13 сентября 2002 г. – М., 2002.*

УДК 621.396:621.391

СИСТЕМЫ ЗАЩИТЫ ОТ МОШЕННИЧЕСТВА И МЕРЫ ПО ПРЕДУПРЕЖДЕНИЮ МОШЕННИЧЕСТВА В ОБЛАСТИ СОТОВОЙ ТЕЛЕФОННОЙ СВЯЗИ

Алексей Марченков, Ярослав Бурыгин
ДСТСЗИ СБ Украины

Анотація: **Рассмотрены способы совершения мошенничества в области сотовой телефонной связи, проведена их классификация. Кратко рассмотрен состав оборудования, которое используется мошенниками и конкретные приборы. Рассмотрены слабые места стандартов сотовой связи, общие методы выявления мошенничества и конкретные реализации систем защиты от различных видов мошенничества, которые в настоящее время используются операторами сотовой связи. Даны**

рекомендации по предотвращению мошенничества против вашего сотового телефона и прослушивания переговоров.
Summary: **The ways of fraud fulfilment in the field of cellular communication and their classification are described in the given article. The structure of the equipment which is used by the swindlers and particular devices are briefly described. The weak places of the standards of cellular communication, general methods of fraud detection, particular realizations of protective systems from various kinds of fraud which are now used by the operators of cellular communication are described. The recommendations for fraud prevention to your cellular phone and listening of negotiation are given.**
Ключові слова: **Сотовая связь, мошенничество, система защиты.**

I Введение

Сотовая телефонная связь является сегодня одним из наиболее динамично развивающихся видов беспроводной персональной связи. Однако значительно большими темпами возрастет преступность в этой сфере. Преступления совершаются организованными преступными группами, деятельность многих из которых носит транснациональный характер.

По данным Ассоциация по борьбе с мошенничеством в области связи ежегодные убытки операторов и абонентов от "двойников" во всем мире составляют более чем 12 млрд. USD.

Точные убытки украинских и российских операторов неизвестны. Типовые потери западного оператора составляют от 3 до 5% от доходов.

Более 1,5 млн. обладателей мобильных телефонов ежегодно отказываются оплачивать выставленные счета. К такому выводу пришла консалтинговая компания Mummert + Partner. По ее данным, только в текущем году немецким компаниям мобильной связи придется списать на безнадежные долги около DM 750 млн, что составляет примерно 3,5% от их годового оборота и в некоторых случаях достигают 40% дохода операторов связи, причем данный показатель особенно высок у молодых поставщиков телекоммуникационных услуг и операторов сотовой связи, а ниже всего он у традиционных операторов фиксированной связи.

Операторы терпят убытки от мошенников также в форме потери доверия абонентов. Увеличиваются и затраты компаний на борьбу с "сотовой преступностью".

Принятые в нашей стране в качестве национальных стандарты сотовой связи NMT-450 и GSM, а также используемые AMPS и DAMPS, существенно различаются по степени их уязвимости. К примеру, аналоговые NMT и AMPS могут быть прослушаны простыми сканерными приемниками.

Но кроме прослушивания переговоров злоумышленник, пользуясь особенностями организации сотовой связи, может теми или иными путями получить доступ к дополнительной информации о подвижной станции.

II Способы совершения преступлений в сфере сотовой телефонной связи

Преступления в сфере сотовой телефонной связи могут быть объединены в две основные группы:

- преступления против операторов сотовой связи (переадресация звонков, мошенничество с абонементом, перепрограммирование, клонирование);
- преступления, посягающие на интересы пользователей сотовой телефонной связи (несанкционированный перехват информации, выявление местоположения пользователя, хищение мобильных телефонов сотовой связи, незаконное использование утерянных и похищенных мобильных телефонных аппаратов).

2.1 Преступления против операторов сотовой связи

Существует несколько типичных схем совершения преступных посягательств данного вида. Рассмотрим их более подробно.

а) Переадресация звонков. Преступник становится клиентом компании мобильной связи, покупает телефон, а затем дает рекламу в газету о предоставлении услуг дешевой связи с любой страной мира. Связавшийся с ним клиент называет номер, с которым он хочет связаться. Затем мошенник вешает свою трубку, устанавливает переадресацию на указанный номер и связь осуществляется в обход через АТС. При этом номер преступника не занят и может использоваться снова. Таким образом, можно одновременно обслужить множество международных вызовов, получить за них деньги и скрыться.

б) Мошенничество с абонементом. Данная преступная схема имела место на Западе и включает следующие стадии.

1. Преступник абонирует сотовую связь на имя другого лица без ведома последнего.
2. Преступник использует телефон в операциях по "торговле телефонными звонками", то есть предлагает своим клиентам анонимно звонить в любое точку мира по низкому тарифу (например, 100 долларов в час).

3. Если счет остается неоплаченным, телефон отключается. Мошенник подключается к очередному чужому номеру.

4. Компании сотовой связи возмещают компаниям междугородной связи стоимость таких звонков.

в) Перепрограммирование. Данная схема предполагает выполнение следующих основных операций.

1. Преступник приобретает сотовый телефонный аппарат законным способом и заменяет микросхему, или же нелегально приобретает телефон с уже перепрограммированным программным запоминающим устройством (ПЗУ).

2. При помощи перепрограммированного аппарата преступник получает доступ к коммутационному оборудованию телефонных компаний, и его вызовы обрабатываются, как и любые другие, с той лишь разницей, что предъявить по ним счет некому.

3. Поскольку компания сотовой связи не может установить личность клиента, она вынуждена оплатить счета по стоимости междугородной части таких вызовов. Если такая махинация проведена на высоком уровне, данный тип мошенничества невозможно отследить или предотвратить.

г) Клонирование. Клонирование основано на том, что абонент использует чужой идентификационный номер (а, следовательно – и счет) в корыстных интересах. При использовании данного способа используется следующая последовательность действий.

1. Преступник перехватывает идентифицирующий сигнал чужого телефона и выделяет из него идентификационные номера ESN (Electronic Serial Number – электронный серийный номер), (MIN, Mobile Identification Number – мобильный идентификационный номер) или IMEI (International Mobile Station Equipment Identity – международный идентификационный номер оборудования подвижной станции). Потенциальный преступник может перехватить эту электронную информацию при помощи радиосканера либо так называемого сотового кэш-бокса, представляющего собой комбинацию сканера, компьютера и сотового телефона. Он легко выявляет и запоминает номера MIN, ESN или IMEI и автоматически перепрограммирует себя на них. Использовав пару MIN/ESN или IMEI один раз, он стирает ее из памяти и выбирает другую. Такой аппарат делает выявление мошенничества практически невозможным. Несмотря на то, что эта аппаратура пока еще редка и дорога, она уже существует и представляет растущую опасность для пользователей сотовой связи.

2. Преступник перепрограммирует свой телефон так, чтобы пользоваться электронным серийным номером и телефонным номером этого абонента. Перепрограммирование осуществляется путем перенесения информации с помощью компьютера на микросхему, которая вставляется в сотовый телефон. Таким телефоном можно пользоваться до тех пор, пока несанкционированные вызовы не будут обнаружены. Стоимость разговора с этого аппарата заносится центром коммутации на счет того абонента, у которого эти номера были украдены.

3. Доказав, что такие вызовы были произведены не им, абонент может опротестовать счета и добиться их отмены. В таких случаях компания сотовой связи вынуждена оплатить междугородную часть таких вызовов. Преступник же выходит на номер любого другого абонента и снова возвращается к своему незаконному бизнесу.

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.

Например, в больших городах Запада, чаще всего в аэропортах, работают мошенники, которые, клонировав ESN-номер чьего-либо мобильного телефона, предоставляют за плату возможность другим людям звонить с этого телефона в отдаленные страны за счет того, чей номер выкрали.

2.2 Преступления против пользователей сотовой телефонной связи

Среди преступлений против интересов пользователей сотовой телефонной связи наиболее опасным является несанкционированный перехват информации, который осуществляется с различными целями, среди которых одна из наиболее значимых – экономический шпионаж.

а) Несанкционированный перехват информации

В настоящее время электронный перехват разговоров, ведущихся по сотовому телефону AMPS, стал широко распространенным явлением. Так, например, в Канаде, по статистическим данным, от 20% до 80% 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. Мобильные сотовые телефоны, особенно аналоговые, являются самыми уязвимыми аппаратами 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 AMPS, может быть прослушан с помощью программируемых сканеров с полосой приема 30 КГц, способных осуществлять поиск в диапазоне 860-890 МГц. Для этой же цели можно использовать и обычные сканеры после их небольшой модификации, которая 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 персонального компьютера.

Используемый в цифровых сотовых телефонах DAMPS алгоритм шифрования Cellular Message Encryption Algorithm (CMEA) может быть вскрыт опытным специалистом в течение нескольких минут с помощью персонального компьютера. Цифровые коды, набираемые на клавиатуре цифрового сотового телефона (телефонные номера, номера кредитных карточек или персональные идентификационные номера PIN) могут быть легко перехвачены с помощью цифрового сканера.

б) Выявление местоположения пользователя

Оставим в стороне такую очевидную возможность, как выявление адреса абонента через компанию, предоставляющую ему эти услуги. Не многие знают, что наличие мобильного сотового телефона позволяет определить как текущее местоположение его владельца, так и проследить его перемещения в прошлом.

Текущее положение может выявляться двумя способами. Первым из их является обычный метод 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 в 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 услуг основана на длительности использования системы. В зависимости от компании эти данные могут храниться от 60 дней до 7 лет.

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

Таким образом, все схемы мошенничества в области сотовой телефонной связи, или фрода (fraud – несанкционированный доступ к услугам сотовой связи, а также получение услуг в режиме неправомочного доступа), можно свести в общую классификацию, которая предлагается западными аналитиками.

III Классификация основных видов мошенничества в области сотовой связи

- **Мошеннический доступ** (access fraud) – несанкционированное использование услуг связи путем перехвата и перепрограммирования серийных ESN, MIN или IMEI идентификационных номеров сотовых телефонов.

В AMPS эти номера могут быть перехвачены при помощи сканера и использованы для программирования других телефонов – метод создания нелегального "двойника". Способ возможен на сетях без аутентификации. Защита основана на проверке записей звонков на предмет обнаружения почти одновременных звонков из разных зон; проверка с использованием "черных списков", а также анализ статистики на "подозрительные события", прежде всего рост трафика абонента.

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

Способ работает, как правило, пока владелец не известит компанию и та не заблокирует доступ с украденного телефона. Защита – блокировка клавиатуры паролем, немедленное заявление в компанию-оператор об утрате телефона, присмотр за телефоном.

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

Способ работает при плохом качестве работы с клиентами, отсутствии предоплаты на счету, а также до момента, когда компания принимает решение о блокировке телефона. Защита – строгий кредитный контроль, введение предоплаты, "горячий биллинг (система оплаты переговоров)" или "онлайн биллинг"; создание базы данных клиентов и контроль заявленной информации; создание "черных списков" недобросовестных клиентов.

- **Хакерское мошенничество** (hacking fraud) – проникновение хакеров в компьютерную систему защиты оператора сотовой связи для удаления механизмов защиты или переконфигурации системы (центра коммутации и базовых станций) в своих целях.
- **Техническое мошенничество** (technical fraud) – неправомочное изготовление (клонирование) телефонных трубок, SIM-карт 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.

IV Оборудование, используемое для осуществления некоторых видов мошенничества в области сотовой связи

Перехват информации в аналоговых сетях, например NMT-450, AMPS, возможен посредством сканерных приемников и интерсепторов. Для измерения параметров современных средств связи используются специальные устройства, например, радиотестеры Stabilock 4015 и Stabilock 4032.

В состав данных приборов входят анализатор спектра, цифровой запоминающий осциллограф, устройство декодирования вызывных последовательностей, генератор сигналов и т. д. Предусмотрены возможности программирования режимов работы, запись программ в память, а также управление от внешнего персонального компьютера.

Универсальный прибор для проверки высокочастотной радиосвязи HP 8920 A/D, в состав которого входят измерители мощности сигналов, цифровой осциллограф, встроенный компьютер, а также устройство проверки сотовой связи с временным разделением каналов, позволяет вести контроль сотовых телефонов, автоматически, проводя их полный параметрический анализ.

Созданные на базе сканерных приемников и управляющих ПК программно-аппаратные комплексы позволяют проводить не только перехват переговоров, но и анализ временных и статистических взаимосвязей между сигналами, индивидуальных особенностей их спектров и модулирующих функций, вести базу радиоэлектронных средств. К ним относятся комплексы типа RS-1100, АРК-ПК 5К, КРОНА-6000 и др.

Малые вес и габариты комплексов в сочетании с универсальным питанием (как от сети, так и от встроенных аккумуляторов) позволяют работать с ними в салоне автомобиля, в стационарных и полевых условиях.

Помимо комплексов, собранных на базе сканерных приемников, могут использоваться и специализированные комплексы.

Программно-аппаратный комплекс "Стрела-DAMPS" позволяет прослушивать и записывать переговоры абонентов стандартов DAMPS-800, AMPS и NAMPS, поддерживает протоколы IS-54 и IS-136. Комплекс работает в режимах сплошного прослушивания всех переговоров или выборочно конкретных абонентов, автоматически отслеживает переход из соты в соту контролируемого абонента, отображает текущее состояние телефона (зарегистрирован в системе, разговаривает, не обнаружен) и т. д.

Одноканальный приемник прямого канала стандартов AMPS/NAMPS и DAMPS "Сонет-800" (выполнен в виде сотовой трубки Motorola) используется для прослушивания разговоров в зоне действия одной базовой станции. Обеспечивает сквозное прослушивание всех или только конкретных абонентов, автоматически отслеживает переход из соты в соту и т. д.

Для декодирования в реальном масштабе времени перехваченных сообщений, закрытых аппаратурой засекречивания, используются специальные устройства, например, 640-SCRD-INT.

Мобильный комплект перехвата помещается в небольшой чемодан и может выглядеть как набор вполне обычных вещей: компьютер-ноутбук, диктофон и специальная приставка, которую неспециалист может принять за блок питания. В зависимости от того, для каких целей планируется использовать оборудование, в комплект могут входить специальный приемник (трансивер), идентификатор, опрашиватель и перехватчик.

Трансиверы позволяют отслеживать уровни сигналов базовой станции и проводить мониторинг или фильтрацию заданных номеров. С их помощью считывается серийный номер мобильного телефона и определяется идентификационный. Об этих номерах не знают владельцы мобильных телефонов: первый - записывается в ПЗУ при его изготовлении на заводе, а второй представляет собой абонентский номер в конкретной сотовой сети связи.

Серийный и идентификационный номера просто определить и при выключенном мобильном телефоне. Достаточно пройти рядом или приблизиться к человеку, у которого находится телефон.

Идентификатор определяет неизвестные сотовые телефоны, сохраняет собранную информацию в памяти, распечатывает ее на принтере, генерирует метку "Дата-Время" и выбирает требуемые телефоны с помощью функции фильтра.

Опрашиватель позволяет прослушивать переговоры и определять вызываемый номер.

С помощью *перехватчика* осуществляется управление от компьютера через интерфейс RS-232.

В свое время эти приборы были специально созданы для проведения исследований в сотовых сетях и обнаружения мошенников, а сегодня они нелегально используются для весьма неблаговидных целей криминальными структурами.

Самым дешевым считается оборудование для прослушивания сотовых телефонов, работающих в стандарте AMPS. Оно стоит всего $18 тыс. Для NMT-450i – $25 тыс., для цифрового DAMPS – $43 тыс. Самый дорогой комплект – для стандарта GSM-900 и 1800. Специалисты называют цифру в $ 1,5 млн. Именно благодаря высокой стоимости данного оборудования GSM считается самым "защищенным стандартом".

V Методы (системы) борьбы против мошенничества в области сотовой связи

Важным направлением борьбы с сотовыми мошенниками сегодня признается совершенствование методов анализа звонков с целью выделения аномального поведения абонентов. На прошедшей в Лондоне в апреле 1998 года ежегодной международной конференции "Борьба с мошенничеством в мобильных системах связи" (Digital Mobile Fraud'98) были рассмотрены системы защиты, построенные на различных принципах.

1) Системы, построенные на задании особых правил контроля и основанные на статистическом анализе звонков

Например, если с интервалом в 1 секунду следуют два вызова, а по учетной записи эти вызовы попадают в различные ячейки (например, в разных концах города), то можно сделать вывод, что происходит нештатная ситуация.

Для предотвращения мошенничества при роуминге предлагается два основных метода – сокращение периода обмена роуминговыми данными до 1 часа и использование специальной сигнализации со схем, которые связаны с коммутаторами, обеспечивающими синхронизацию по роумингу, для получения в режиме on-line информации о вызовах, которые делает абонент в сети другого коммутатора. Другая схема основана на возможности классифицировать роуминговые звонки по стране проживания клиента. Если он приехал, скажем, из России, то можно предполагать, что он будет связываться, в основном, со своей страной, а не с Нигерией. Предложено ввести в биллинговую систему некоторую классификацию стран, наиболее подверженных мошенничеству, – например, страны Юго-Восточной Азии. При вызовах именно в эти регионы система защиты от мошенничества начинает более тщательно отслеживать поведение клиента.

2) Системы, построенные на принципах теории распознавания образов

Подобные системы защиты строят различные адаптивные схемы, которые позволяют создать некоторый многомерный образ поведения абонента. При получении каждого следующего звонка этот образ перестраивается. Если клиент начинает вести себя аномально, слишком много говорить или делать слишком длинные вызовы, его образ поведения начинает значительно отличаться от уже созданного, и модель не может к нему подстроиться. Это служит сигналом, что с клиентом что-то не то.

3) Самообучающиеся системы, построенные на принципах нейронных сетей

Система нейронного типа внешне очень похожа на адаптивные системы, но отличается способом реализации. В этом случае все построено не на чисто математической модели, а на некоторой самообучающейся программе, которая имитирует поведение нейронных сетей в мозге человека. Такие системы способны даже отличать телефонные вызовы мошенников от внешне похожих звонков легальных абонентов.

VI Некоторые конкретные реализации систем защиты от мошенничества в области сотовой связи

PhonePrint (Corsair Communications Inc.) – комплекс распознавания радиотелефонов по радиоотпечаткам – Radio Frequency Fingerprint (уникальным характеристикам излучения передатчика каждого аппарата).

Представители оператора Fora Communications (AMPS, Санкт-Петербург), где PhonePrint был установлен в июле 97 года, утверждают, что система компании Corsair в целом работала успешно (стоимость составила около 1 млн. USD), однако уже в 98 году систему решили демонтировать и возвратить компании-производителю. Около 1/3 клиентов, отказавшихся от услуг Fora, испытывали неудобства от "двойников" с клонированными аппаратами. Fora вместо этого установила систему A-Key.

По-видимому, следует ожидать вспышек "фрода" на региональных системах, куда "перетекут" клоны из С.-Петербурга.

В 98.07 система PhonePrint введена в действие в Казахстане на системе Алтел.

В 98.11 данная система была поставлена компанией Ericsson в Малайзию на сеть ETACS (55% сотового рынка).

В 99.01 Corsair подписал соглашение с Comcel (Colambia) на поставку системы PhonePrint 5.0, которая позволяет одной системой антифрода обслужить сразу несколько систем сотовой связи.

В 99.02 состоялось подписание договора с ALLTEL – американским мультиоператором, обслуживающим более 6.5 млн абонентов в 22 штатах. Если абонент данной сети переходит в режим роуминга, например, отправившись в другой город (при условии, что там также имеется система PhonePrint(R) 5.0), то местная система отправит "радиоотпечатки" излучения телефона в его "домашнюю систему". Связь состоится только в случае, если и роминговая система и "домашняя система" будут располагать однотипной информацией. Если отпечатки совпадут, то звонок можно будет сделать.

Несмотря на сложность сети, ожидание соединения для клиента не увеличивается, в то время, как любителей позвонить за чужой счет ждут трудные времена.

Система AKEY (A-Key) это тривиальное название системы аутентификации, используемой в сетях AMPS/DAMPS. Собственно AKEY представляет себой восьмибайтовое число-ключ, хранящееся в сотовом телефоне абонента и являющееся уникальным для каждого абонента. AKEY вводится при продаже телефона клиенту и хранится в базе. AKEY не меняется и остается постоянным при нормальной работе телефона. На основе AKEY (постоянный ключ) с помощью хеш-функции CAVE, использующей в качестве входных параметров, помимо AKEY, ESN, MIN телефона также случайное число, присланное по эфиру с базовой станции, каждый раз генерируется новый временный ключ, называемый SSD_A (тоже 8 байт). Этот ключ в дальнейшем и используется при аутентификации для генерации ответного значения. Постоянный AKEY не используется при аутентификации и служит только для расчета временного ключа. При установлении соединения система передает сотовому телефону случайное число, которое шифруется по алгоритму CAVE (Cellular Authentication and Voice Encryption) с использованием временного ключа SSD_A и других уникальных параметров телефона (ESN, MIN) в качестве ключа. Ответ посылается на базовую станцию, которая, в свою очередь, независимо от телефона генерирует ответное число (все параметры телефона, в том числе и AKEY, и текущий SSD_A, хранятся в базе на станции), и сравнивает его с полученным. В случае несовпадения числа, принятого от телефона с независимо посчитанным числом, аутентификация считается неудачной и телефону отказывается в соединении. Периодически (примерно раз в неделю) станция посылает сотовому телефону сообщения о генерации нового временного ключа, SSD_A. По получении этого сообщения (SSD_UPDATE) телефон рассчитывает новый временный ключ SSD_A, используя уже известный постоянный AKEY, ESN, MIN, и случайное число со станции. Таким образом, сам ключ аутентификации (SSD_A) является временным и периодически меняется. Поэтому становится бессмысленным "клонирование" трубок (а также нахождение SSD_A методом последовательного перебора), поскольку после первого же изменения ключа работать дальше будет только один телефон с новым ключом.

Система SIS. SIS – Subscriber Identification Security. Внедрение началось на сетях NMT450 с системы "Дельта Телеком" еще в 1994 году. С тех пор, как утверждает менеджмент компании, не зарегистрировано ни одного случая проникновения в сеть. Внедрение функции было сложным и дорогостоящим и включало:

- модернизацию аппаратного и ПО коммутатора;
- приобретение и внедрение аппаратно-программного комплекса;
- замену всех мобильных аппаратов, не имевших встроенной функции SIS;
- модификацию ПО базовых станций.

Соответствующая реализация стандарта известна под названием NMT450i. Помимо функции защиты от фрода, оператор получает ряд дополнительных возможностей, например, пониженный тариф для телефона с

ограниченной (одной сотой) мобильностью, ограничение зоны обслуживания для конкретного абонента, SMS и ряд других. Основное преимущество – возможность организации автоматического роуминга.

Принцип действия SIS аналогичен AKEY: при запросе на соединение станция посылает сотовому телефону случайное число, которое обрабатывается хеш-функцией SIS в телефоне с использованием 120-битового уникального ключа пользователя. Часть результата хеш-функции посылается на базовую станцию для сравнения, другая часть используется для шифрования набираемого номера. В отличие от AKEY, SIS не меняется и всегда остается постоянным для конкретного телефона, а также обеспечивает шифрование набираемого номера (в системе AKEY тоже предусмотрена возможность шифрования номера, однако она не используется в российских системах). Также, в отличие от AKEY, SIS-код зашивается в телефон производителем и не может быть изменен провайдером услуг (AKEY обычно может вводится с клавиатуры). Есть информация о том, что некоторые “специалисты”, которые сняли матрицу чипа SIS, теперь могут легко подделывать эти коды.

Система CMG. Введена в действие на системе "Белсел" (Белоруссия, NMT-450). Предназначена для защиты информации на сотовой сети, будет соединена с базой данных более 30 000 абонентов "Белсел". Проведено сопряжение "Белсел" с "Сотел" (Россия).

Система FraudBuster. Система обнаружения фрода и формирования профиля абонента предназначена для обнаружения и борьбы в том числе и с новыми видами фрода. Система, выбранная на 99.01 уже 27 сотовыми компаниями в мире, способна накапливать данные о вызовах каждого конкретного абонента и создавать на этой основе индивидуальные профили каждого абонента. Они затем дополняются, анализируются по мере совершения новых звонков и способны немедленно обнаруживать аномальную активность, которая может свидетельствовать о факте фрода.

Поскольку система защиты не связана с концепцией построения инфраструктуры системы сотовой связи, то она подходит практически для всех систем GSM, AMPS, CDMA, TDMA, iDEN.

Система Signature Fraud Management System (Signature FMS) от Lucent Technologies – новое ПО, которое может использоваться операторами, как проводной, так и беспроводной связи. Система способна динамически в реальном времени оценивать отклонения в поведении абонентов с целью обнаружения действий, характерных для злоумышленников.

Данная система защиты также не связана с концепцией построения инфраструктуры системы сотовой связи, она также подходит практически для всех систем сотовой и проводной связи.

Что касается клонирования сотовых телефонов, то в войне с компаниями-производителями оборудования мошенники в области сотовой связи сдают свои позиции. В настоящее время практически отсутствуют сотовые системы, для которых возможно клонирование: AMPS/DAMPS (без числа-ключа A-Key), NMT-450 (без SIS-кода).

Зашифрованные данные абонента GSM, хранящиеся в небольшой смарт-карте, называемой также модулем идентификации пользователя (SIM – Subscriber Identification Module), пока обеспечивают однозначную аутентификацию пользователя и надежное шифрование данных по алгоритму с открытым ключом (RSA).

О клонировании телефонов стандарта GSM путем перехвата информации в эфире данных нет. Однако известен способ создания клонов путем физического доступа к SIM-карте и перезаписи хранящейся в ней информации в другой модуль (или его эмулятор). Так, есть информация, что в начале 2002 года специалисты по безопасности корпорации IBM обнаружили серьёзную уязвимость в защите SIM-карт сотовых телефонов стандарта GSM. Об этом сообщил сайт Vnunet.com.

Воспользовавшись этой дырой злоумышленник всего за пару минут может подобрать PIN-код, "клонировать" SIM-карту и говорить за чужой счет.

Методика взлома, обнаруженная специалистами IBM, состоит из 7 шагов. Чтобы узнать секретные коды телефона, нужно проанализировать прохождение электрических импульсов через SIM-карту.

Для взлома телефона необходимо получить к нему полный доступ на 1–2 минуты. Впрочем, в IBM подчеркивают, что уязвимы к такому взлому лишь SIM-карты первого поколения и что их методика является, скорее демонстрацией возможности взлома и пока не представляет очень уж большой опасности.

VII Рекомендуемые меры по предотвращению мошенничества против вашего сотового телефона

- держать документы с ESN-номером вашего телефона в надежном месте;
- ежемесячно и тщательно проверять счета на пользование сотовой связью;
- в случае кражи или пропажи сотового телефона сразу предупредить фирму, предоставляющую вам услуги сотовой связи;

- держать телефон отключенным до того момента, пока вы не решили им воспользоваться. Этот способ самый легкий и дешевый, но следует помнить, что достаточно одного выхода на связь, чтобы выявить MIN/ESN номера аппарата;
- регулярно менять через компанию, предоставляющую вам услуги сотовой связи, MIN-номер вашего аппарата;
- наиболее эффективным методом противодействия является шифрование MIN/ESN номера (вместе с голосовым сигналом) по случайному закону. Этот метод дорог и пока малодоступен.

VIII Рекомендуемые меры по предупреждению несанкционированного перехвата информации с вашего сотового телефона

Для предотвращения перехвата информации специалисты рекомендуют пользователю предпринять следующие меры:

- использовать общепринятые меры по предупреждению перехвата и раскрытия информации: избегать или свести к минимуму передачу конфиденциальной информации, такой как номера кредитных карточек, финансовые вопросы, пароли; использовать в этих целях более надежный проводной телефон, убедившись, что собеседник не использует в этот момент радиотелефон; не использовать сотовые или беспроводные телефоны для ведения деловых разговоров;
- 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 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;
- использовать системы связи, в которых данные передаются с большой скоростью при частой автоматической смене частот в течение разговора;
- использовать цифровые сотовые телефоны.

Ну, а что же есть на вооружении у самого пользователя мобильного телефона? Пока ему доступны только аналоговые и цифровые устройства кодирования речи – скремблеры (на их использование в Украине требуется разрешение Департамента специальных телекоммуникационных систем и защиты информации СБ Украины), но и это не мало. Эти устройства универсальны и могут быть установлены в любой аппарат, если в нем есть место для установки платы.

Самые распространенные среди них – цифровые скремблеры компании Selectone – имеют более 260 миллионов кодов, а такие модели, как TVS-2 компании Midian, – свыше миллиарда.

Для того, чтобы не искать приставок, можно приобрести мобильный телефон сразу со встроенным скремблером. Однако при этом не стоит все же забывать об общедоступных мерах предосторожности при проведении переговоров.

Кардинально решить проблему можно, став абонентом Национальной системы конфиденциальной связи, работы над созданием которой в настоящий момент ведутся специалистами Департамента специальных телекоммуникационных систем и защиты информации СБ Украины. Вопросы обеспечения конфиденциальности переговоров и защиты от “двойников” будут заложены в НСКЗ на системном уровне и реализованы с использованием высокостойких алгоритмов шифрования.

Статья подготовлена по материалам, полученным из Интернет и размещенных на российских и украинских сайтах.

УДК 638.235.231

СКОРОСТЬ СВЕТА: ОТ НУЛЯ ДО БЕСКОНЕЧНОСТИ

Юрий Арепьев
Национальный технический университет Украины “КПИ“
НИЦ “ТЕЗИС” НТУУ “КПИ“

Аннотация: **Бурное развитие систем коммуникации с необходимостью ставит вопрос об увеличении скорости передачи информации, верхняя граница которой, исходя из установленных на сегодняшний день знаний, не может превышать скорости света в вакууме. В последнее время предпринимаются настойчивые попытки выйти (если такое возможно) за эту границу. Цель**