Лабораторная работа № 3

Исследование методов защиты абонентского терминала в системе сотовой связи GSM

3.1. Цель лабораторной работы:

Ознакомление с методами защиты абонентского терминала в системе сотовой связи GSM.

Перед выполнением лабораторного задания студенты должны ориентироваться в основных аспектах информатики и иметь основные понятия о функционировании системы сотовой связи GSM.

В результате выполнения лабораторного задания студенты должны получить навыки защиты защиты абонентского терминала в системе сотовой связи GSM.

3.2. Краткие теоретические сведения

SIM-карты.

SIM-карты являются неотъемлемыми частями сотовых телефонов GSM, однако телефоны многих других стандартов вполне обходятся без них. ″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). Пока первые сети создавались одной фирмой, проблем не возникало, но с ростом числа производителей сотовых телефонов ситуация усложнилась. Разнобой буквенно-цифровых систем обозначения заводских номеров аппаратов приводил к тому, что при любой замене телефона абоненту обязательно надо было ехать с ним в отдел обслуживания сотовой компании и регистрировать его

там. В начале 90-х годов двадцатого века разработчики "общеевропейского" цифрового стандарта сотовой связи GSM решили эту проблему. Ими было предложено разделить функции идентификации оборудования и абонентов.
Для идентификации телефонов в стандарте GSM используется специальный 15-значный уникальный номер - Международный Идентификатор 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 информацией. Параметры же абонента вынесены в специальный сменный модуль - Subscriber Identity Module (SIM), вставляемый в телефон (по сути SIM-карты представляют собой адаптированную под нужды мобильной связи разновидность смарт-карт).

Код оборудования IMEI используется для проверки "легальности" телефонов - сотовая сеть отказывает в обслуживании "незаконным" (например, украденным) аппаратам, чьи номера значатся в специальном "стоп листе". Обмен номерами "подозрительных" телефонов может производиться непосредственно между сотовыми сетями, для разрешения обслуживания легальных телефонов нет необходимости в какой-либо их регистрации в сети, и абонент может самостоятельно менять телефоны по своему усмотрению. Проверка кода IMEI в сетях GSM не является обязательной процедурой и поддерживается далеко не всеми компаниями.
Именно в результате этого обстоятельства в мире и существует подпольный рынок торговли ворованными телефонами GSM.
SIM-карты 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. SIM-карта помимо идентификационного номера абонента содержит функции связанные с проверкой подлинности карты (аутентификацией) и шифрованием переговоров, что обеспечивает безопасность.

Таким образом, функции, выполняемые в других стандартах непосредственно телефоном, в GSM поделены 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.

Необходимость выполнения в SIM-карте операций по обработке информации определила реализацию ее по принципу смарт-карты работающей под управлением операционной системы и содержащей: процессор, узлы ввода и вывода информации, а также RAM и EEPROM (содержит всю прикладную информацию - как пользовательскую, так и служебную), ROM память. В SIM-картах реализуются многие другие функции: записные книжки телефонных номеров с именами, списки последних сделанных и принятых вызовов и т. п. В телефоны, поддерживающие стандарт GSM 2+ (модели после 1998 г.), встроена 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.… Такая автоматизация ускоряет пользование такими услугами как: 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.

SIM-карта блокируется специальным кодом персонального идентификатора абонента - Personal Identification Number - PIN (защищает телефон от несанкционированного использования посторонними людьми). 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, 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. После десяти ошибочных попыток ввода PUK24 SIM-карта блокируется полностью и требуется ее замена. Если же снятие блокировок проходит успешно, то значение PIN-кода может быть в любой момент изменено самим пользователем. Ключ PUK изменению не подлежит. Кроме кодов PIN и PUK существует также аналогичная пара кодов PIN2 и PUK2 (тоже содержится в документации на SIM-карту, получаемой 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.

Иногда на телефоны устанавливается блокировка 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. 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 является замена программного обеспечения.
Особый вопрос составляет стойкость SIM-карт против взлома. Именно для противодействия подобным попыткам, вся служебная часть перепрограммируемой памяти SIM-карты построена так, что информация из нее доступна только внутреннему процессору SIM-карты. "Взлом" SIM-карты методом прямого подбора необходимых номеров достижим лишь в случаях, когда карта на длительное время попадает в руки злоумышленников. 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 взлом SIM-карт на основе анализа побочных каналов утечки информации является достаточно эффективным.
Карты, подобные SIM-картам стандарта GSM, используются в UMTS (USIM карты) и IDEN телефонах, в мобильной спутниковой связи ("Инмарсат мини-М", "Иридиум", "Глобалстар" "Турайя") и в терминалах сетей высокоскоростного беспроводного доступа по технологии Wi-Fi. Разработки аналогичных карт имеются и

для стандартов cdmaOne (IS-95) и CDMA2000 - R-UIM-карты (Removable User Identity Module - съемный модуль идентификации пользователя). Далее рассматривается безопасность систем GSM, где важную роль играет SIM-карта.

3.3. Лабораторное задание

При подготовке к лабораторному занятию следует предварительно изучить: методы защиты мобильного терминала (т.е. сотового телефона и смартфона) от клонирования и несанкционированного доступа в сеть (ввод PIN-кода, PIN-кода, доступ к мобильному терминалу при неправильном вводе пин-кода путем использования PUK-кода, определение IMEI по данным на мобильном терминале, а также по специальному коду доступа для данного мобильного терминала).

1. Используя конкретный мобильный терминал в соответствующем меню ввести заведомо неправильный PIN-код и удостовериться, что допуск к работе с мобильным терминалом отсутствует.
2. Ввести правильный PIN-код и изменить его текущее значение на другое (удостовериться, что допуск к работе с мобильным терминалом обеспечивается).
3. При наличии PUK-кода для используемой SIM-карты ввести три раза неправильный PIN-код и удостовериться, что допуск к работе с мобильным терминалом отсутствует. После этого ввести PUK-код для разблокировки мобильного терминала.
4. Определить по данным мобильного терминала указанный на нем код IMEI.
5. Определить реальный код IMEI, введя специальную для данной модели служебную комбинацию.
6. Удостовериться, что значения этих кодов совпадают.

ПОРЯДОК ВЫПОЛНЕНИЯ ЗАНЯТИЯ

При выполнении задания рекомендуется соблюдать следующую последовательность:

1. Изучить методические указания к данному лабораторному занятию.
2. Определить все исходные PIN-, PUK-коды, а также доступ к коду IMEI.

3. Выполнить лабораторную часть
4. Ответить на контрольные вопросы.

СОДЕРЖАНИЕ ОТЧЕТА

1. Краткие теоретические сведения по методам кодовой защиты мобильного терминала.
2. Выполненное задание.

3.4. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое SIM-карта?
2. Что такое PIN-, PUK- и IMEI-коды и их назначение?
3. Как изменить PIN-код?
4. Как получить доступ к терминалу при неправильном вводе PIN-кода?
5. Как определить код IMEI?
6. Как определить достоверность данной модели терминала?

3.5 Библиографический список

3.5.1.Основная литература

1.Методические указания к данной лабораторной работе.

2. Конспект лекций.

3.5.2. Дополнительная литература

1. Основы теории радиоэлектронной борьбы. /Под ред. Николенко Н.Ф. М. Военное издательство, 1987. -196 с.
2. Осипов А. С. Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП : учебник / А.С. Осипов ; под науч. ред. Е.Н. Гарина. - Красноярск : Сиб. федер. ун-т, 2013. - 344 с.
3. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. Учеб. пособие. –М.: РГГУ, 2002.-399 с.
4. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Инфокоммуникационная безопасность открытых систем: Уч. Для вузов. В 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. М.: Горячая линия – Телеком, 2006. – 536 с.

5. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФМГГУим. М. А. Шолохова, 2009. – 372 с.: ил.
6. Варфоломеев А.А. Основы информационной безопасности: Учеб. пособие. – М.: РУДН, 2008. – 412 с.: ил.