Вопросы безопасной передачи данных

при использовании GSM-канала

Во многих современных системах безопасности в качестве основного или резервного канала передачи данных применяется GSM/GPRS/EDGE-канал. Это неудивительно, поскольку GSM-устройства могут передавать данные везде, где есть покрытие сотовой связи, а скорость передачи сегодня достигает вполне приемлемых значений. Например, технология EDGE позволяет передавать данные со скоростью до 384 кбит/с. В реальности скорость оказывается в несколько раз ниже, но для мобильных устройств этого вполне достаточно. Определившись с выбором технологии передачи данных, следует рассмотреть немаловажный вопрос о безопасности канала. Какие сложности могут возникнуть при работе GSM-устройства M2M и можно ли обезопасить передаваемые по эфиру данные?

Всеволод Нестеров
Олег Пушкарев
wireless@compel.ru

Для нарушения работы GSM-модема существуют так называемые GSM «глушилки». Существует большое количество подобных устройств, которые отличаются методами подавления, выходной мощностью и стоимостью. Профессиональные «глушилки» стоимостью до от 1 до 10 тысяч евро применяют интеллектуальное подавление, в то время как простейшие устройства стоимостью в несколько сотен евро являются простейшими узкополосными генераторами шума. Первые применяют сигналы, ничем не отличающиеся от сигналов базовых станций, и распознать наличие этих «глушилок» практически невозможно; вторые просто генерируют шум в определенном диапазоне частот, и распознать наличие таких «глушилок» вполне по силам современным GSM-устройствам. Обнаружение глушения не означает возможность передать данные каким-то «волшебным» способом. Однако после того как устройство определило, что его «глушат», оно может использовать резервные каналы передачи данных или выполнить определенные защитные действия, например включить звуковую сигнализацию тревоги.

Во многих случаях интерес злоумышленника заключается не в нарушении работы GSM-устройства, а в получении доступа к передаваемым данным. Каким образом можно обеспечить безопасность данных на этапе передачи от GSM-устройства до базы данных клиента на удаленном сервере?

Как видно на рис. 1, передача осуществляется по четырем областям: радиоинтерфейс от GSM-устройства к базовой станции оператора, инфраструктура провайдера, Интернет и локальная сеть клиента. Наиболее незащищенными областями являются сегмент передачи пакетов по эфиру от мобильного устройства к базовой станции оператора и область Интернета. Сегмент передачи данных от мобильного устройства к базовой станции имеет следующие слабые стороны:

- Активные атаки: GSM-оборудование может подвергаться атакам оборудования, имитирующего работу базовых станций.
- Ограниченная область шифрования: предназначена для фиксированных сетей.
- Прослушивание канала: помогает шифрование, но некоторые сети шифрование не поддерживают.
- Невозможность определения достоверности данных: такие алгоритмы не предусмотрены.
- Односторонняя аутентификация: происходит аутентификация только пользователя в сети, невозможна идентификация сети пользователя.
- Слабый алгоритм шифрования: длина ключа слишком короткая, в то время как скорость вычислений увеличивается. Используемый

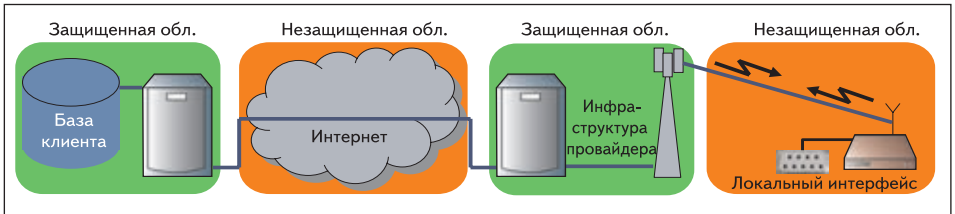

Рис. 1. Области передачи данных

Рис. 2. Использование SSL-тоннеля в области Интернета

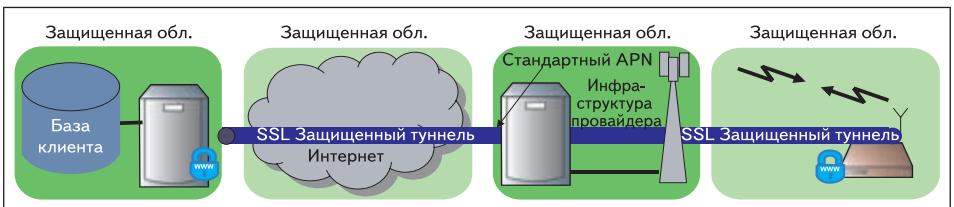

Рис. 3. Защита информации при использовании Security Plugin компании Wavecom

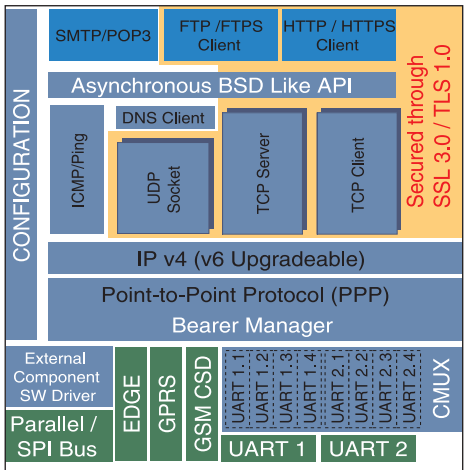

Рис. 4. Структура беспроводного процессора Wavecom

алгоритм шифрования COMP 128 в настоящее время взломан, а замена оборудования с новыми алгоритмами слишком сложна.
- Не обеспечивается скрытность идентификации терминала: IMEI-номер не скрывается.
- Отсутствие возможности отслеживания шифрования и политики безопасности провайдера: нет индикации шифрования, нет индикации политики безопасности в роуминге.

Если устройство имеет некий локальный интерфейс, например UART, то злоумышленник может подсоединиться к этому интерфейсу и, подав какие-либо AT-команды, нанести вред или получить доступ к данным внутри GSM-устройства. Таким образом, локальный интерфейс и область передачи до базовой станции нельзя считать защищенными. Инфраструктура провайдера между базовой станцией и файрволом или прокси-сервером считается безопасной, так как получить доступ к этой области проблематично, то же касается и области сервера клиента. Что касается Интернета, то эта область тоже не защищена, так как продвинутый «хакер» в состоянии получить доступ к интернет-данным. Методом борьбы с хакерскими атаками на этапе передачи данных через Интернет является использование SSL — криптографического протокола, обеспечивающего безопасную передачу данных по сети. В этом случае провайдер должен поддерживать эту услугу и выдавать клиенту специальный адрес APN. Как правило, эта услуга является платной, и провайдер взимает ежемесячную абонентскую плату. Таким образом, незащищенной остается только область «воздушного интерфейса» — при передаче данных от мобильного устройства к базовой станции (рис. 2).

Производитель беспроводных GSM-процессоров (GSM-модулей) — компания Wavecom — выпускает для своих продуктов специальные программные модули (plugins), с помощью которых можно решать различные прикладные задачи, например выполнять шифрование данных. Для популярных GSM-процессоров Q2686/Q2687 предлагается специальное ПО «Security Plugin» — набор программных средств для обеспечения защиты данных. При использовании этого набора возможна реализация защиты данных в области «воздушного интерфейса», а также использования SSL-шифрования для Интернета без участия провайдера, соответственно и без абонентской платы (рис. 3).

Рассмотрим более подробно этот набор программных средств. Все модемы и модули Wavecom производитель позиционирует как беспроводные процессоры. Это означает, что продукт Wavecom представляет собой мощный процессор на архитектуре ARM7 или ARM9, наделенный GSM-функциональностью, то есть возможностью передавать данные через сеть GSM. Производитель бесплатно предоставляет среду разработки OPEN AT и другие программные средства, с помощью которых можно написать собственное приложение на языке C, скомпилировать его и «залить» в модем или модуль. После запуска приложения беспроводной процессор может самостоятельно выполнять какие-либо действия: анализировать входы, передавать данные по GSM-каналу, анализировать входящий поток данных на порт и т. д. Внутренняя структура беспроводного процессора Wavecom с использованием протокола SSL представлена на рис. 4.

Стек SSL для беспроводных процессоров Wavecom имеет следующие характеристики:
- SSL 3.0/TLS 1.0 совместимость, создан на базе OpenSSL версии 0.9.7;
- поддержка аутентификации (клиент и сервер), шифрования, проверка достоверности данных, защита от подмены сообщений;
- поддержка мультисессий;
- независимость от аппаратной несущей (GPRS, SPI, UART);
- ключи к шифру: RSA-алгоритм, алгоритм Diffie-Hellman;
- схемы аутентификации: RSA, DSS, NULL;
- алгоритмы шифрования: DES, утроенный DES, RC2, RC4, NULL;
- алгоритмы хеширования: MD5, SH1;
- поддержка HTTPS, FTPS.

Механизм шифрования данных в модулях предусматривает хранение ключа как внутри беспроводного процессора в разных частях Flash-памяти, так и вне устройства, и загрузку ключа с внешнего процессора или из внешней памяти.

В ПО “Security Plugin” предусмотрена также возможность работы с несколькими операторами сотовой связи, данный функционал носит название “Open SIM Access”. Это, например, позволяет повысить надежность передачи данных при перемещении мобильного объекта по территории разных стран, где может просто не оказаться работающей сети нужного оператора. Работу с несколькими SIM-кар-

Рис. 5. Работа с несколькими SIM-картами

тами можно использовать и для сокращения расходов на трафик, выбирая оптимальный тариф для данной местности, времени суток, локального или междугороднего звонка и т. п. Дополнительные SIM-карты подключаются через имеющийся второй канал UART или другие интерфейсы (SPI, USB). Для преобразования сигналов последовательного интерфейса в сигналы управления SIM-картой используется дополнительная микросхема TDA 8029 (NXP).

Для того чтобы злоумышленники не получили доступ к памяти беспроводного процессора, разработан функционал "Crypto Engine", который предусматривает возможность шифрования хранимых данных и защиты этой области памяти от несанкционированного доступа. Даже если «хакер» напишет свой код и внедрит его в беспроводной процессор, он не сможет получить доступ к защищенной области Flash-памяти без специальной авторизации: процессор просто перезагрузится, и причина перезагрузки будет сохранена в памяти.

Компания Wavecom также предоставляет технологию "in SIM", которая позволяет избавиться от необходимости использования физических SIM-карт в том виде, в котором мы их используем сейчас. Вместо SIM-карты в виде пластика используются только входящие в них кристаллы, содержащие необходимую для регистрации в сети провайдера информацию. Данные кристаллы на фабрике Wavecom разваривают в корпус обычной микросхемы, которая затем запаивается на плату беспроводного процессора, как обычный радиоэлемент. При этом остается возможность работы и с внешней SIM-картой. Встроенная SIM-карта позволяет существенно повысить надежность работы GSM-устройства в условиях предельных температур или механических воздействий. Кроме того, это позволит избежать несанкционированного использования SIM-карты, например для частных телефонных звонков. Внедрение технологии "in SIM" на практике требует совместной работы компании-оператора, Wavecom и производителя SIM-карт. Существует две бизнес-модели внедрения этой технологии в конечное изделие разработчика. В первой Wavecom заключает договор с компанией-оператором и устанавливает контакты с производителем SIM-чипов, во второй производитель конечного продукта самостоятельно заключает договор с оператором, получает кристаллы от производителя SIM-карт и передает их в Wavecom для установки в беспроводные процессоры.

Еще одна программная новинка Wavecom — встроенный в "Security Plugin" алгоритм обнаружения работы неинтеллектуальных средств радиоглушения, а также непроизвольного подавления несущей вследствие интерференции других радиоэлектронных средств. Этот алгоритм базируется на измерении уровня сигнала и синхронизации во время процедуры сканирования сети. Во время этой процедуры получаются несколько промежуточных результатов измерения, которые позволяют пользователю предпринять какие-либо профилактические действия, если это необходимо. Результат выдается как вероятность радиоглушения (таблица).

Таблица

Вероятность	Описание
Нулевая	Нет подозрения на глушение. Радиоэфир рассматривается как нормальный
Низкая	Низкая вероятность глушения. Некоторые параметры радиоэфира рассматриваются как ненормальные
Средняя	Средняя вероятность глушения. Большая интерференция радиоспектра
Высокая	Высокая вероятность глушения. Радиоэфир рассматривается как сильно зашумленный, но есть вероятность того, что беспроводной процессор сможет синхронизироваться с сетью
Радиоэфир заглушен	Радиоэфир заглушен, синхронизация с сетью невозможна, большой уровень сигналов на многих частотах

Заключение

Рассмотренные возможности беспроводных процессоров Wavecom, обладающих современными средствами защиты информации, позволяют использовать их в самых ответственных приложениях для систем безопасности и платежных систем. Новое программное обеспечение «Security Plugin» позволяет защитить передаваемые данные, как в радиоканале, так и в памяти беспроводного процессора, обнаружить факт глушения и повысить общую надежность системы благодаря функциям встроенной SIM-карты и поддержки нескольких SIM-карт.