АНАЛИЗ УЯЗВИМОСТЕЙ УСТРОЙСТВ МОНИТОРИНГА ПОДВИЖНЫХ ОБЪЕКТОВ. РАЗРАБОТКА ПРОТОТИПА, ЗАЩИЩЕННОГО ОТ ЭТИХ УЯЗВИМОСТЕЙ

А. В. Цыкарев
Пермский государственный национальный исследовательский университет,
614990, Пермь, Букирева, 15

Работа посвящена изучению и разработке устройств для мониторинга подвижных объектов. В рамках данного исследования меня интересовал аспект безопасности обрабатываемых в таких устройствах, данных.
В рамках данной работы были поставлены следующие задачи:

- анализ распространенных уязвимостей устройств мониторинга подвижных объектов;
- разработка прототипа устройства, защищенного от этих уязвимостей.

Анализ работы устройств, выявление возможных каналов утечки информации. Принципиальная схема работы большинства устройств мониторинга подвижных объектов приведена на рис. 1.

Рис. 1. *Общая схема работы устройств мониторинга подвижных объектов*

В данной работе рассмотрены уязвимости, возникающие при: получении данных от спутников, их передаче на сервер с помощью GSM, уязвимости, обусловленные наличием возможности удаленного конфигурирования. Уязвимости в работе сервера не рассматриваются.

Уязвимости при получении информации о местоположении от спутника. Джон Уорнер (Jon Warner) из Национальной лаборатории Аргон совместно со своими коллегами провел исследование уязвимостей GPS-

трекинга [1]. В своем исследовании Уорнер обозначил следующий вектор атаки: передавать на устройство ложные данные о местоположении, заставляя его принимать их за действительные.

В ходе работы Уорнер с коллегами вывел набор признаков, которые помогут определить, что устройство подвергается атаке.

1) Чрезмерно высокий уровень сигнала;
2) Одинаковый уровень сигнала от разных спутников;
3) Низкий уровень шума в сигнале;
4) Несоответствие текущего местоположения номерам видимых на данный момент спутников.

Исходя их выработанных в ходе проведенного исследования Джона Уорнера признаков атаки и возможностей аппаратной платформы конкретного устройства можно вовремя выявить атаку и передать данные о её наступлении на сервер. Оператор получив эти данные сможет вовремя предпринять необходимые действия и предотвратить нежелательные последствия.

Уязвимости при передаче данных о местоположении на сервер при помощи GSM. Данные о местоположении объекта передаются от устройства на сервер при помощи GSM. Все передаваемые данные шифруются. На сегодняшний день передаваемые с помощью GSM данные шифруются с использованием алгоритмов шифрования семейства A5.

Еще в 2009 году, как сообщает издательство The New York Times [2], немецкий криптолог Карстен Нол (Karsten Nohl) продемонстрировал способ взлома алгоритма A5/1. Также, состоялась публичная демонстрация взлома на конференции Chaos Communication Congress в Берлине. Вся информация по проекту взлома и таблицы для кодовых книг A5/1 сегодня можно найти в открытом доступе.

Так как данные передаваемые с помощью GSM могут быть перехвачены, и, как выяснилось, могут быть расшифрованы за считанные часы – при разработке устройств мониторинга подвижных объектов необходимо учитывать этот факт. Для обеспечения дополнительной защиты всех передаваемых данных необходимо организовать дополнительное шифрование данных.

Анализ возможных уязвимостей при удаленном конфигурировании устройств. Для анализа возможных уязвимостей был исследовано устройство мониторинга отечественной компании RusLink модели NAVIXY A2. При очном осмотре устройства была обнаружена маркировка «GV500». При попытке найти информацию по данному запросу удалось выйти на сайт зарубежного производителя Queclink. «Queclink GV500» - устройство, продаваемое данным производителем. Очевидно, что оно же импортируется в Россию и продаётся под брендом «NAVIXY A2». Имея эту информацию удалось найти описание протокола для конфигурирования устройства SMS-командами.

Все команды для конфигурирования защищены паролем. Но, по умолчанию на устройствах установлен стандартный пароль «gv500». Таким обра-

зом для изменения конфигурации устройства, нам достаточно знать номер телефона установленной в нём сим-карты. Требования к командам (не более 160 символов) и обилие различных параметров в каждой из них не предоставляют нам возможность установить пароль достаточной длины.

Наиболее эффективным способом защиты от подобного рода атак является реализация «доверенного списка» номеров. Т.е. в устройство заведены определенные номера, с которых возможна обработка конфигурационных сообщений. Сообщения с других номеров – игнорируются.

Проектирование и разработка устройства, защищенного от основных уязвимостей. Для разработки устройства была использована платформа Arduino. Использованные компоненты:

1. Iteaduino UNO V1.0 (ATmega 328). Дешевый аналог Arduino Uno. Наследует все функции Arduino.
2. EFCom GPRS/GSM Shield V1.2. Модуль совместимый с Arduino. Управляется AT-командами
3. GPS Shield V1.1. Модуль совместимый с Arduino. Позволяет получать данные о местоположении по GPS.

Устройство пытается получает данные о местоположении по GPS (задействован GPS Shield V1.1). Если получены валидные данные - происходит GET-запрос к веб-серверу (задействован EFCom GPRS/GSM Shield V1.2). В запросе передаются следующие данные: широта, долгота, скорость, идентификатор клиента.

Используемая аппаратная платформа Arduino накладывает следующие ограничения:

1. Размер загружаемой прошивки ограничен 32 Кб. Таким образом использование больших алгоритмов (например, SSL).
2. 2 Кб ОЗУ. Это ограничивает максимальный размер строк, с которыми мы можем работать

Исходя из всех вышеизложенных ограничений для реализации дополнительного шифрования данных был выбран блочный алгоритм шифрования XTEA. Он имеет длину ключа 128 бит. К тому же, для Arduino существует специальное решение в виде дополнительной библиотеки, которое позволяет реализовать данный алгоритм.

Для реализации наиболее безопасного механизма конфигурирования необходимо используется проверка телефона отправителя конфигурационного сообщения. Формат принимаемых СМС: **DT:<PASSWORD>:<кол-во секунд>.** Если сообщение в указанном формате поступает с «доверенного номера» - меняется интервал отправки данных устройством на сервер.

В прошивке устройства используется библиотека TinyGPS, которая предоставляет нам возможность работать с NMEA сообщениями, которые основная плата получает от GPS модуля. Получаемые устройством в этих сообщениях данные (координаты местоположения, дата, время, скорость, направление движения, высота, кол-во спутников в поле видимости) не позволили в полной мере использовать признаки подмены сигнала, выявленные

Джоном Уорнером. Для реализации проверки на ложный сигнал спутников был использован параметр с количеством видимых на данный момент спутников. В программном коде условие срабатывания тревоги звучит так «Если кол-во видимых спутников изменилось более чем на 3». Данная проверка происходит каждые 60 секунд работы устройства. В случае срабатывания данной проверки – происходит отправка запроса на сервер с информацией о срабатывании тревоги.

Результаты. Были выявлены и проанализированы некоторые из существующих на сегодняшний день уязвимости устройств мониторинга подвижных объектов. Также, были рассмотрены варианты борьбы с этими уязвимостями. Неотъемлемой частью работы была разработка прототипа устройства, которое было бы защищено от данных уязвимостей. Работы над разработкой прототипа завершились успешно.

Список литературы

1. *Jon S. Warner, Ph.D. and Roger G. Johnston, Ph.D., CPP Vulnerability Assessment Team Los Alamos National Laboratory Los Alamos, New Mexico, 87545* GPS Spoofing Countermeasures
2. *http://www.nytimes.com/, Published: December 28, 2009* Cellphone Encryption Code Is Divulged
3. *Shanghai SIMCom wireless solutions Ltd.* SIM900_AT Command Manual_V1.03
4. *iteadstudio.com, 2012-04-07* Arduino GPS shield 1.1
5. *iteadstudio.com, 2012-11-11* Iteaduino UNO