Вопросы безопасности LPWAN систем

Конференция "Вызовы цифровой экономики и требования государства: найти баланс"

Александр Шептовецкий

Эксперт Ассоциации Интернета Вещей

14.02.2018.

Классификация удаленных атак на распределенные информационные системы

По характеру воздействия

- пассивное
- активное

По цели воздействия

- нарушение конфиденциальности информации
- искажение информации
- нарушение работоспособности системы

По наличию обратной связи с атакуемым объектом

- однонаправленная атака
- с обратной связью

По условию начала осуществления воздействия

- атака по запросу от атакуемого объекта
- атака по наступлению ожидаемого события на атакуемом объекте
- безусловная атака

Преимущества LPWAN – дополнительный источник угроз безопасности

Преимущества LPWAN

- батарейка
- дальность
- стоимость

Ключевая особенность LPWAN – физический уровень доставки информации

- Радио интерфейс ISM радиоканал – открытый для всех
- Энергетика бита - короткие информационные посылки
- Топология звезда – не симметричная система связи

Источники угроз

- Легкость доступа к физическому каналу передачи данных
  - ISM диапазон
  - большой радиус действия
  - доступность оборудования
- Открытые стандарты
- Ограничения в объеме передаваемой информации
- Крайне ограниченные возможности обратного канала
- Открытое ID конечного устройства

Любой «пионер» может поиграть с вашей информацией

Специфика информационного потока

Малый объем полезной информации от основных LPWAN объектов (конечных точек)

- Кнопка-триггер - 1 бит
- Датчик-счетчик - 2 байта
- Трекер - 4 байта

Первоочередные задача защиты информации в LPWAN сетях – это обеспечить:

1. доставку
2. целостность
3. подлинность
4. защиту от повтора
5. Конфиденциальность

Информации от большинства конечных точек может быть совсем не конфиденциальной, но обязательно должна быть достоверной

Сначала достоверность, затем конфиденциальность

Возможные атаки на физический уровень на примере сигнализаций

История автомобильного брелока.

- статический код
- динамический код (Клиффорд, KeeLog)
- диалоговое кодирование (запрос «свой-чужой»)

Массовое применение

- KeeLoq — блочный шифр на регистре сдвига

с нелинейной обратной связью NLFSR

(Non-Linear Feedback Shift Register).

Однонаправленный протокол.

Имеет массовое использование у производителей автомобилей и дополнительных охранных систем

- Спутниковые системы (GPS+GSM)

Массовый интеллектуальный взлом

- Сканеры
- Код грабберы
- Глушилки сигнала

Массовое применение рождает массовый взлом

Анализ атак на автосигнализации

Варианты успешных атак

- Простое вскрытие KeeLoq, если знать код производителя, одинаковый для определенного класса систем, что позволяет создать "мануфактурные" кодграбберы.
- Подмена кода. Используются физические особенности передачи кода по радиоканалу, глушится небольшой кусок сигнала от брелока, при этом злоумышленник получает информацию, а штатный приемник нет, при повторе сообщения ситуация повторяется, но злоумышленник подсовывает приемнику старое сообщение, а последнее сохраняет у себя для снятия системы с охраны.
- Глушение канала (GSM, GPS, радиоуправление)
- Использование уязвимостей сервисных функций (замена брелока, сервисный режим, что делать если потерял)

Актуальный список взломанных кодграбберами сигнализаций - около 120 наименований, включая практически все штатные сигнализации. Большая часть из этого списка – системы с Keeloq с дискредитированным кодом производителя

Алгоритм Keeloq до сих пор не взломан — взломаны его неудачные реализации.

Анализ защиты существующих LPWAN систем

Элементы защиты существующих LPWAN систем на примере LoRaWAN

- Ключ аутентификации приложения AppKey (ключ устройства)
- Сетевой ключ NwkSKey (**проверка целостности** каждого сообщения используя MIC, AES-128)
- Ключ приложения AppSKey (**шифрования полезной нагрузки**, AES-128)
- Конечное устройство и сетевой сервер после процедуры активации инициализируют два счетчика – счетчик кол-ва переданных фреймов и счетчик кол-ва принятых фреймов

Позволяют эффективно защитить:

- целостность
- подлинность
- защиту от повтора
- конфиденциальность

Расплата – удлинение посылки минимум +12 байт к полезной информации, на которую будет тратится энергия батарейки

Оставшиеся угрозы

- Открытый ID в эфире (возможен мониторинг активности; если Конечная точка типа кнопки-триггера, то сам факт передачи ID и есть сообщение; можно пробовать реализовать атаку с подменой кода как у автосигнализаций)
- Глушение канала связи
- Глушение избранного конечного устройства (как у автосигнализаций)

При массовом распространении, дьявол может скрываться в деталях.

Видение будущего

Совершенствование существующих LPWAN технологий

- Защита LoRa от глушения и постановки точечных помех (у SigFox и Стриж ситуация гораздо лучше)
- Возможное объединение технологий LoRa и SigFox – передача uplink в формате SigFox (Стриж), а downlink в формате LoRa (максимально используются сильные стороны каждой технологии)
- Создание шлюзов между LPWAN и системами малого радиуса действия (Bluetooth, ZigBee, Z-Wave…), например, в виде ретрансляторов для закрытия мертвых зон LPWAN, увеличения его покрытия и удешевления и миниатюризации конечных устройств
- Защита открытого в эфире ID конечных устройств
- Подключение к безопасным распределенным системам сбора, хранения и коммерческой реализации информации, основным на принципах блокчейна, например, таким как IOTA:
  - Достоверная информация
  - Открытое доступное всем хранение идентификаторов событий
  - Конфиденциальность самой информации
  - Низкая стоимость обслуживания события

Будущее IoT рождается сейчас

Спасибо за внимание!