Программно-аппаратные платформы Интернета вещей и встраиваемые системы

Лекция 7

Мини-проекты

- Учитываются в итоговой оценке с весом 0,2 (+2 балла на экзамене)
- Решается «реальная» задача (или хотя бы похожая на реальную)
- Обязательно использование радио (LoRa, IEEE 802.15.4, BLE, WiFi; последние – **не в виде внешних модулей**, управляемых AT-командами)
- Минимум два пункта из списка:
  - Датчик, подключенный по I2C, SPI или аналогичному интерфейсу;
  - GPS-модуль;
  - АЦП;
  - ШИМ;
  - ЖК-дисплей (можно текстовый);
  - Нетривиальный backend (просто положить данные в БД и показать в Grafana не выйдет)

Доклады

- 10-15 минут
- Темы, не затронутые в лекциях:
  - RISC-V – особенности архитектуры, порт RIOT, основные отличия от Cortex-M;
  - 6LoWPAN over BLE;
  - ZigBee;
  - Нейросети на микроконтроллерах, CMSIS-NN;
  - Электрофизиологические измерения;
  - …
- Можно рассказать о «проектной работе», если она укладывается в тематику курса

БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ – ОБЩИЕ ВОПРОСЫ

Модель угроз в радиосети

- Любой желающий может слушать эфир на любой частоте
- В лицензируемом диапазоне любой желающий может передавать в эфир что угодно, пока не придет Роскомнадзор
- В безлицензионном диапазоне любой желающий может передавать в эфир что угодно сколько угодно
- Большинство IoT-систем работает в безлицензионных диапазонах
  - 433 МГц, 868 МГц, 2450 МГц

Модель угроз в радиосети

- Перехват данных
- Передача фальсифицированных данных
- Косвенное определение состояния передающего устройства

«Наивный» протокол

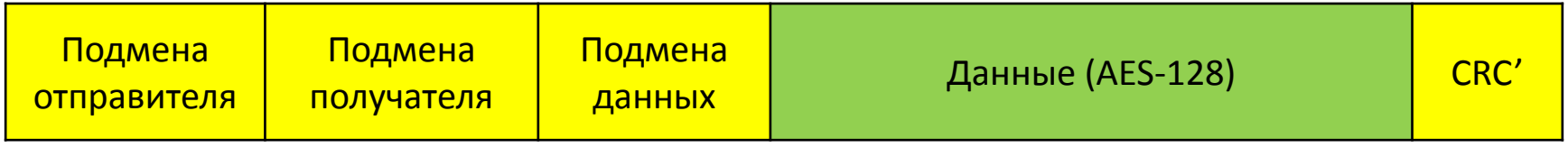
Адрес отправителя	Адрес получателя	Служебные поля	Данные	CRC

- Целостность пакета проверяется контрольной суммой (CRC)
- Данные не зашифрованы
- Любой может прочитать данные
- Любой может сфальсифицировать данные

«Наивный» протокол

- Целостность пакета проверяется контрольной суммой (CRC)
- Данные зашифрованы, например, AES-128
- Посторонний не может прочитать данные
- Посторонний не может сфальсифицировать данные

Подмена данных MAC-уровня



- Принимаем из эфира чужой пакет
- Меняем что угодно, кроме данных (мы не знаем ключа AES-128)
- Пересчитываем контрольную сумму
- Те же данные, но от другого отправителя или к другому получателю, или с другими командами MAC-уровня

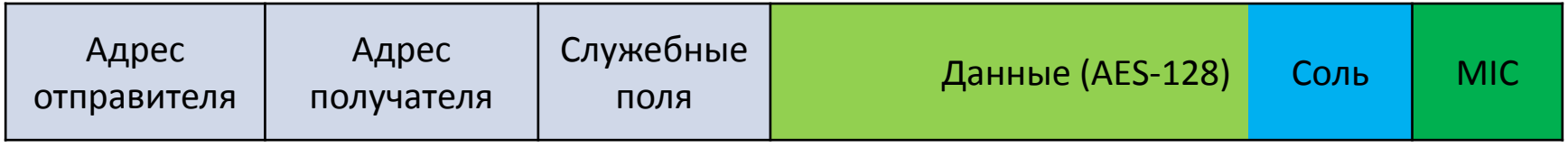
Защита от фальсификации MAC-уровня

- Шифрование всего пакета слишком ресурсоемко
- Вместо контрольной суммы используем MIC (Message Integrity Code, *имитовставка*) – зависящую от ключа однонаправленную хеш-функцию
- AES-CMAC и другие подобные алгоритмы

Определение состояния устройства

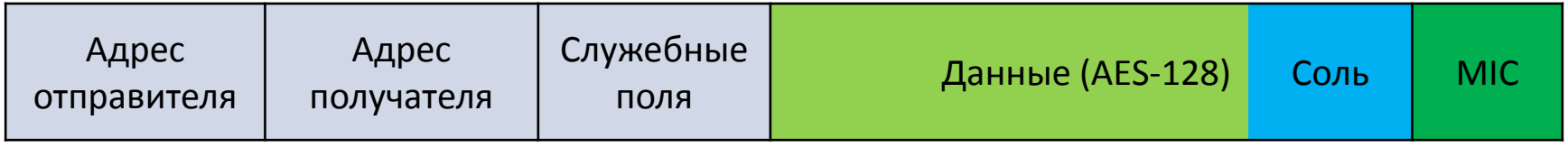
- Шифрование AES-ECB: каждый раз один и тот же ключ
- Зашифрованный блок меняется, только если меняются исходные данные
- Не расшифровывая блок, можно понять, изменились ли входные данные
  - Пример – водосчетчик; если данные не меняются в течение недели – в квартире никого нет

Добавляем «соль»



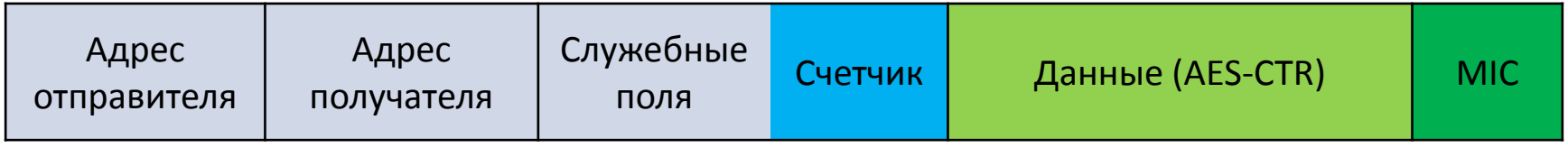
- Добавляем к данным «соль» (salt) – 16- или 32-битное случайное число, каждый раз разное
- При приеме и расшифровке «соль» отбрасывается
- Одни и те же данные, но разная «соль» - различные зашифрованные блоки

Атака повтором



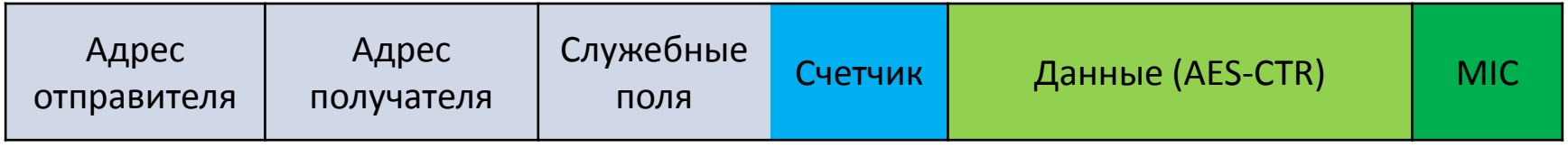
- Прослушиваем эфир, записывая нужный пакет
- В нужный нам момент времени воспроизводим этот пакет
- Например: датчик вскрытия окна
  - записываем пакет «окно закрыто», передаваемый раз в минуту
  - вскрываем окно, глуша радиоэфир
  - выключаем датчик, продолжаем передавать пакет «окно закрыто» сами

Защита от атаки повтором



- Добавляем к MAC-уровню счетчик пакетов
- Счетчик должен только возрастать!
- Сброс счетчика в ноль – отдельная и редкая процедура (Join в LoRaWAN)
- Блочный шифр для данных используется в режиме «со счетчиком» (AES-CTR)

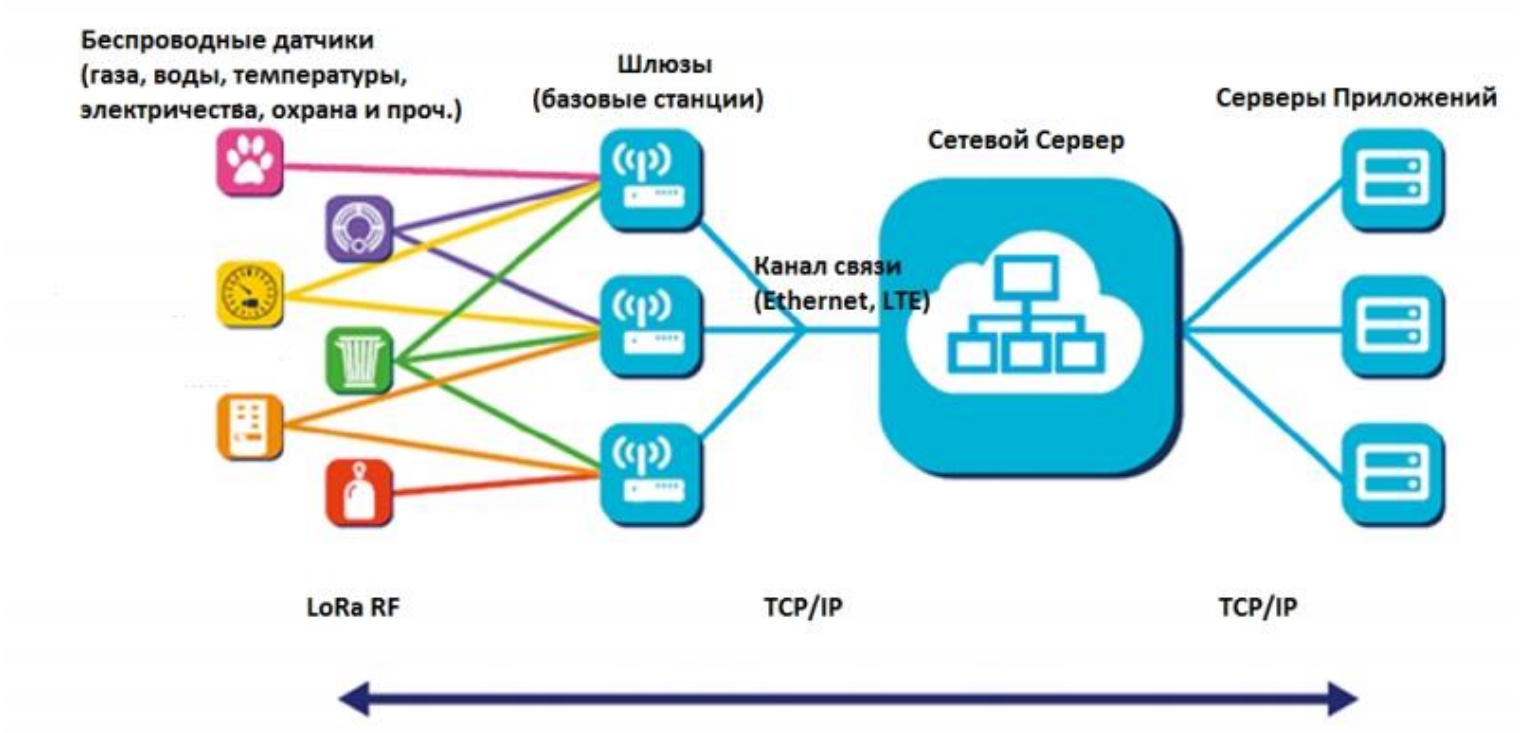
Активная атака повтором



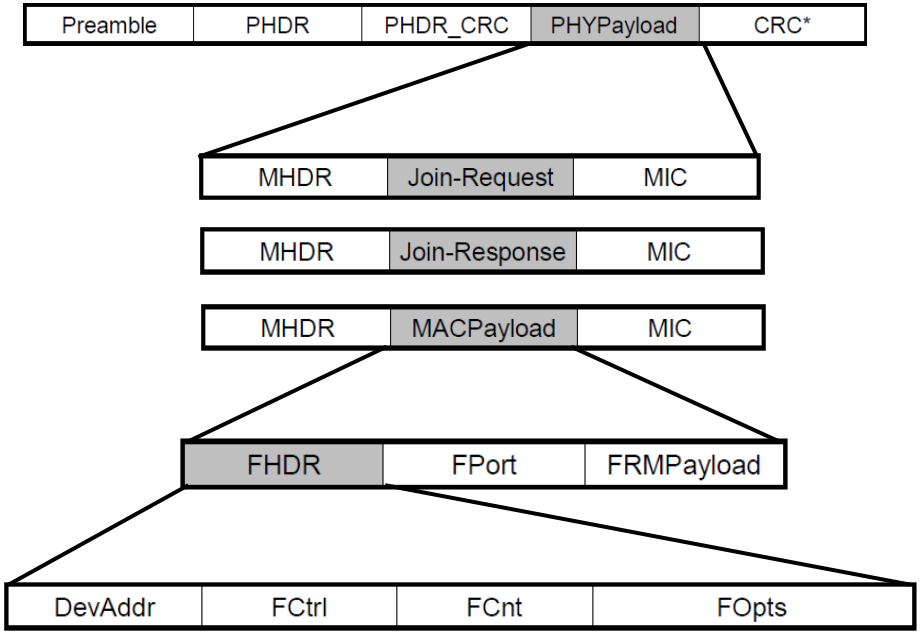
- Записываем пакет с номером n, одновременно поставив помеху приемнику
- При повторной передаче данных записываем пакет с номером n+1, ставим помеху приемнику и тут же передаем записанный пакет с номером n
- Передаем записанный пакет с номером n+1, открываем машину, уезжаем…

БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ НА ПРИМЕРЕ LORAWAN

LoRaWAN – архитектура сети



Пакеты в LoRaWAN



- Преамбула – 12 «чирпов»
- PHDR – заголовок PHY с параметрами модуляции
- Контрольная сумма (CRC) только для uplink

- MHDR – MAC Header, 1 байт с типом сообщения и версией протокола
- MIC – Message Integrity Code, вычисляется по алгоритму AES-CMAC с использованием ключа сети (Network Session Key)
- Payload зашифровано с помощью ключа приложения (Application Session Key)
- FCnt – счетчик кадров

LoRaWAN - безопасность

- Есть шифрование данных приложения (ключ приложения неизвестен серверу сети)
- Есть защита от подмены служебных полей (AES-CMAC с использованием ключа сети)
- Есть защита от атак повтором (счетчик и AES-CTR)
- В ПНСТ LoRaWAN предлагалось использовать шифрование ГОСТ на уровне приложений; текущая версия ПНСТ 516-2021 не предъявляет требований к алгоритмам *шифрования* (*кодирования*?)

LoRaWAN - безопасность

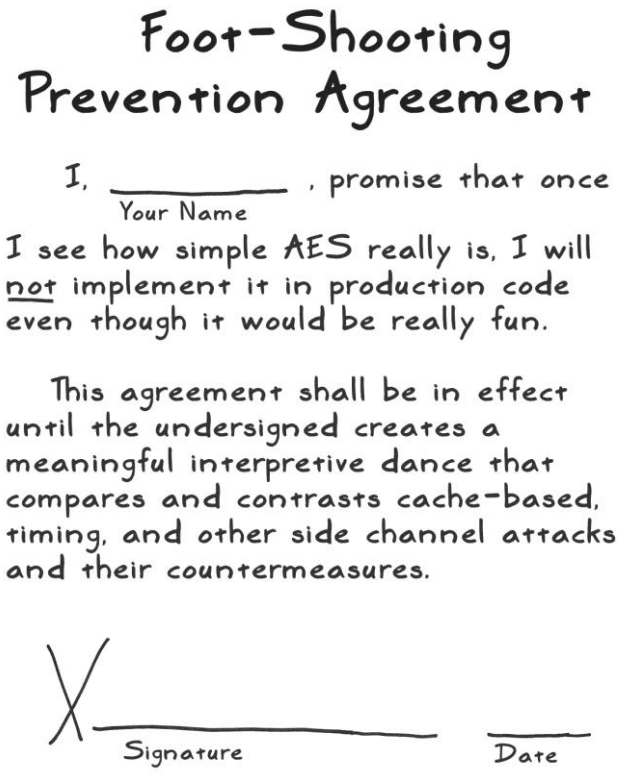
- Активация – обнуление счетчика и выработка двух ключей (Network Session Key, Application Session Key)
  - ABP – Activation by Personalisation
    - Сессионные ключи «зашиты» в устройство, счетчик никогда не обнуляется
    - Невозможно сменить сессионные ключи при их компрометации
    - Проблема: 16- или 32-битный счетчик
  - OTAA – Over-the-air activation
    - Для получения сессионных ключей нужен обмен кадрами Join-Request и Join-Response, при этом обнуляются счетчики кадров
    - Нужен один «зашитый» в устройство ключ (Application Key)
    - При компрометации сессионных ключей их можно сменить

Процедура Join в сети LoRaWAN

НЕКОТОРЫЕ ПРАКТИЧЕСКИЕ ВОПРОСЫ

Три главных правила криптографии

1. Не изобретайте свой алгоритм
2. Если вам кажется, что авторы известных алгоритмов что-то сделали неправильно, но про это не написано у Брюса Шнайера — вам кажется
3. Ни при каких обстоятельствах не изобретайте свой алгоритм



Foot-Shooting Prevention Agreement

I, _____ , promise that once
Your Name
I see how simple AES really is, I will not implement it in production code even though it would be really fun.

This agreement shall be in effect until the undersigned creates a meaningful interpretive dance that compares and contrasts cache-based, timing, and other side channel attacks and their countermeasures.

X _____ _____
Signature Date

Средства операционной системы

- **`sys/crypto`** — криптографические алгоритмы
- **`sys/hashes`** — хеши, в т.ч. криптографические
- **`sys/random`** — генератор **псевдо**случайных чисел

True Random Number Generator

Настоящий генератор случайных чисел может быть только аппаратным:

- подбрасывание монеты
- вращение рулетки
- физические процессы, корнями уходящие в квантовую механику
  - дробовой шум
  - туннелирование электронов

(Pseudo) Random Number Generator

- Сложная числовая функция, выдающая *почти* непредсказуемую последовательность чисел с очень большим периодом
- **Если не сказано иного — всегда предполагайте *псевдо*случайность**
- Последовательность определяется одним числом — *seed*
- При одном и том же *seed* — одна и та же последовательность
- Seed должен быть *настоящим* случайным числом!

Инициализация PRNG

- Источники «настоящих» случайных чисел обычно медленные
- Удобно получить одно случайное число и использовать его, как seed для PRNG
- Источники случайности приемлемого качества:
  - действия пользователя в интерактивной системе
  - потребление ресурсов в многозадачной системе
  - микрошум на «висящем в воздухе» входе АЦП
  - шум в радиоэфире
  - “Jitter” двух тактовых генераторов
- Источники случайности **неприемлемого** качества:
  - время, прошедшее с включения микроконтроллера
- Улучшение качества случайного числа:
  - собрать много приемлемых случайных чисел
  - посчитать для них криптографический хеш (например, SHA-256)