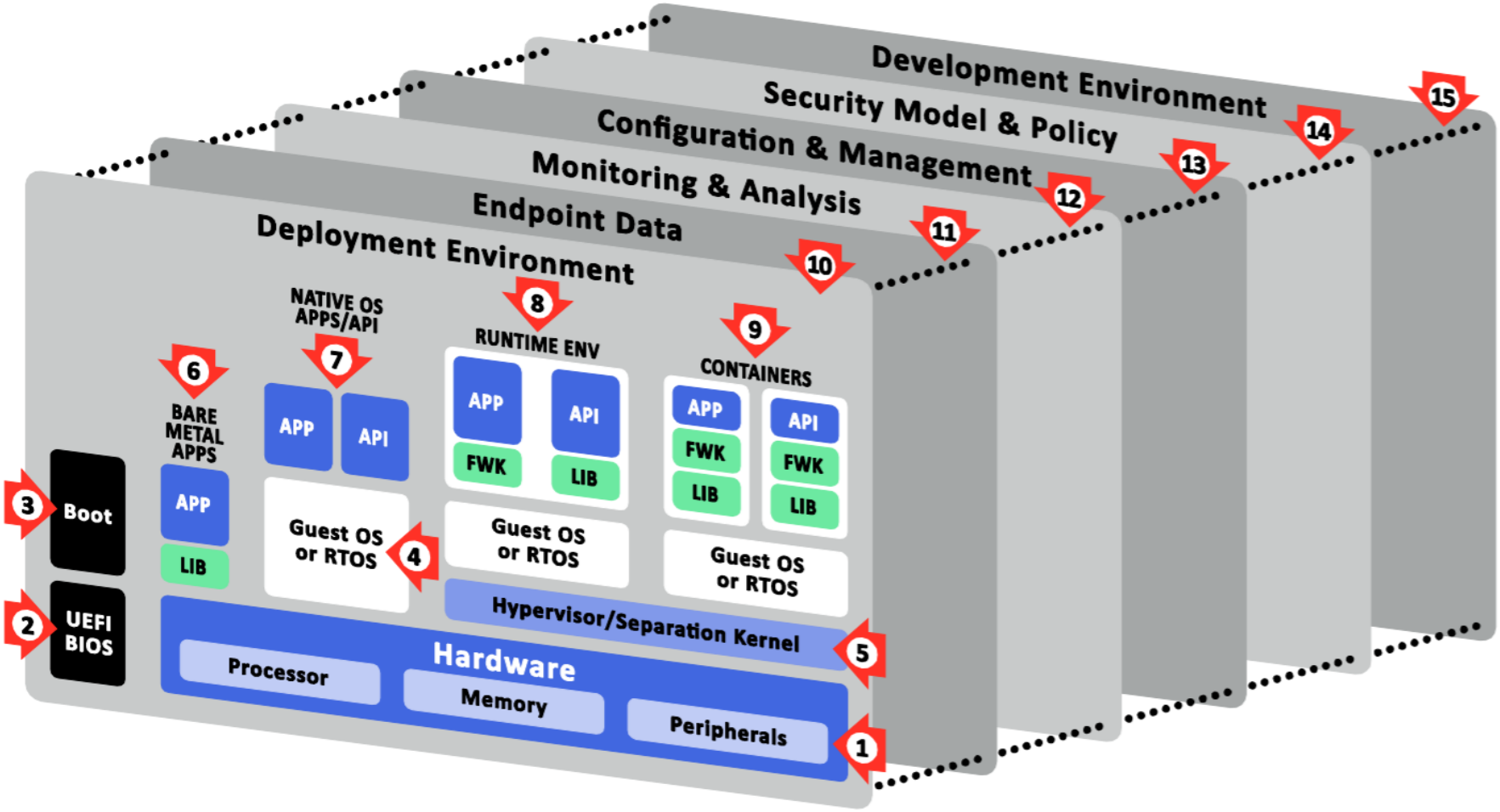
Вопросы реализации механизмов защиты IIoT-устройств

Парьев Сергей

ТБ Форум 2020

Ростелеком
Солар

Угрозы безопасности IIoT-устройства



Ростелеком
Солар

IIC Security Framework, https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Угрозы безопасности IIoT-устройства

- (1) Угрозы, связанные с непосредственным доступом к аппаратуре
- (2)(3) Угрозы, связанные с уязвимостями процесса начальной загрузки
- (4)(5) Угрозы, связанные с уязвимостями в системном ПО
- (6)(7)(8)(9) Угрозы, связанные с уязвимостями в прикладном ПО
- (10) Угрозы, связанные с уязвимостями процесса установки (развертывания) ПО
- (11) Угрозы, связанные с доступом к данных устройства
- (12) Угрозы, связанные с уязвимостями процесса мониторинга
- (13) Угрозы, связанные с уязвимостями процесса управления и конфигурирования
- (14) Угрозы, связанные с уязвимостями в политиках и моделях безопасности
- (15) Угрозы, связанные с уязвимостями процесса разработки

Ростелеком
Солар

Уязвимости компонентов АСУ ТП. Отчет за первое полугодие 2019 года.

Типы уязвимостей

Если проанализировать уязвимости по типам, то первая тройка оказалась вполне ожидаемой: это управление доступом, разглашение информации и инъекции. За ними следуют уязвимости, которые относятся к реализации криптографических функций безопасности. Уязвимости, связанные с отказом в обслуживании, занимают третье место по популярности.

Долевое распределение по типам уязвимостей получается следующее:

28%
уязвимостей связаны с управлением доступом

Рисунок 3. Типы уязвимостей

Наиболее часто, в 28% случаев, в ПО и оборудовании выявлялись уязвимости, связанные с управлением доступом, — так, в большинстве исследованных решений были обнаружены проблемы с аутентификацией и авторизацией. Также эксперты «Лаборатории» нашли в исследованном ПО и оборудовании уязвимости, позволяющие повысить привилегии, а в ряде случаев — полностью обойти механизмы аутентификации и авторизации.

10

Ростелеком
Солар

https://rt-solar.ru/events/news/1728/

Типичные уязвимости IIoT-устройства

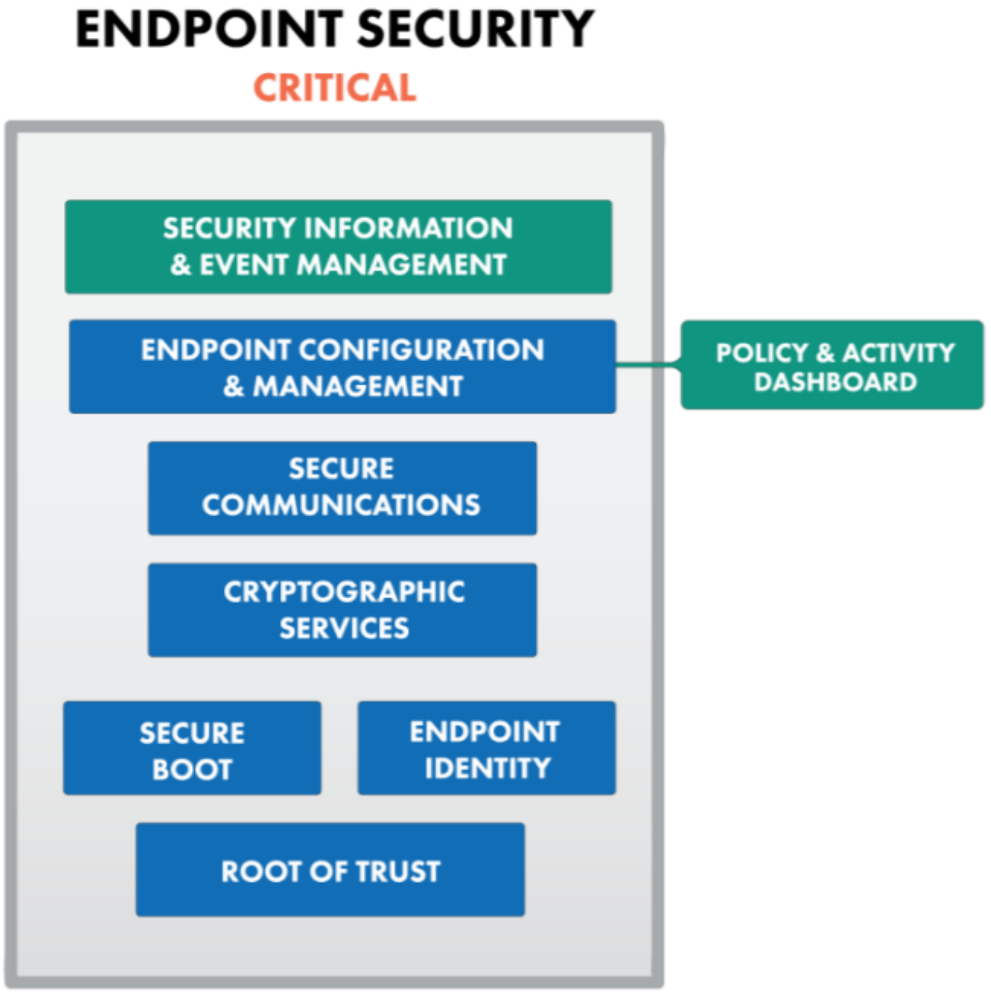
- Уязвимости, связанные с управлением доступом
  - “Вшитые” ключи, пароли и учетки
  - Слабость механизмов аутентификации
  - Возможность обхода аутентификации
- Незащищенная передача данных
- Разнообразные инъекции в web интерфейсах устройств
- Разглашение информации
- Отказы в обслуживании
- Проблемы работы с памятью (переполнения)

Ростелеком
Солар

Что делать?

- Построить процесс разработки безопасного ПО
- Описать:
  - бизнес-процессы
  - схемы развертывания компонентов изделия/решения
  - внутреннюю архитектуру компонентов изделия/решения (включая аппаратные)
  - данные (категории данных, хранилища, сценарии использования, потоки данных)
- Выбрать требования по безопасности (в том числе информации)
- Построить модель угроз (желательно: как самого изделия, так и более крупной системы для использования в которой предназначено изделие)
- Выбрать механизмы защиты, исходя из модели угроз
- Реализовать механизмы защиты

Механизмы защиты



Ростелеком
Солар

IIC Endpoint Security Best Practices, https://www.iiconsortium.org/pdf/Endpoint_Security_Best_Practices_Final_Mar_2018.pdf

Физическая безопасность

- Шкафы
- Корпус
  - Вандальная защита
  - Защита от вскрытия
- Физические ключи
- Внешние кнопки
- Неиспользуемые физические интерфейсы
- Отладочные интерфейсы
- ЭМ излучение, цепи питания

Root of Trust (RoT, “Корень доверия”)

- Использование криптографии
- Необходимая (но не до статочная) основа для построения “доверенной” вычислительной среды
- Доверие к “корню доверия” обычно основывается на сторонних процессах (разработки, производства, распространения, монтирования, развертывания, обслуживания и др.)
- Доверие к любому элементу вычислительной платформы основывается на цепочке доверия, идущей от “корня доверия”
- В виде чего может быть:
  - Основной “секретный” ключ устройства
  - Корневой сертификат (открытый ключ) центра доверия
  - +Защищенное хранилище
  - +Функции обработки запросов
  - +Отдельная защищенная вычислительная среда

Механизмы защиты (1)

- Аутентификация/идентификация (стойкая)
  - Самого устройства во внешних системах
  - Пользователей устройства
- Контроль доступа
  - Модель доступа (субъекты, объекты, права, политики и др.)
  - Механизмы контроля доступа
- Защищенные коммуникационные протоколы
  - TLS
  - OPC UA
- Логирование (событий безопасности)
  - “черный ящик”
- Мониторинг
- Шифрование данных

Ростелеком
Солар

Механизмы защиты (2)

- Контроль целостности вычислительной среды
  - Доверенная (начальная) загрузка
  - Доверенные обновления
  - Управление конфигурациями
  - Контроль запуска приложений
    - “Белые списки” (white listing)
  - Целостность файловых систем (и др. хранилищ данных)
  - Изоляция процессов
    - Виртуализация
    - Контейнеризация
  - Run-time контроль памяти
    - ASLR (рандомизация адресного пространства)

Проблемы развития

- Отсутствие обязательных требований для IIoT-устройств
- Отсутствие/недостаток требований в отраслевых СТО
- Отсутствие готовых методик и практик применения механизмов защиты
- Отсутствие готовых аппаратных компонентов (RoT) с ГОСТ-овой криптографией
- Недостаток готовых программных компонентов для встраиваемого применения, реализующих типовых механизмы защиты
- Недостаток встраиваемых ОС с готовым набором механизмов защиты
- Вопросы сертификации и применения встроенных СКЗИ
- Вопросы сертификации и применения встроенных СЗИ

Контакты

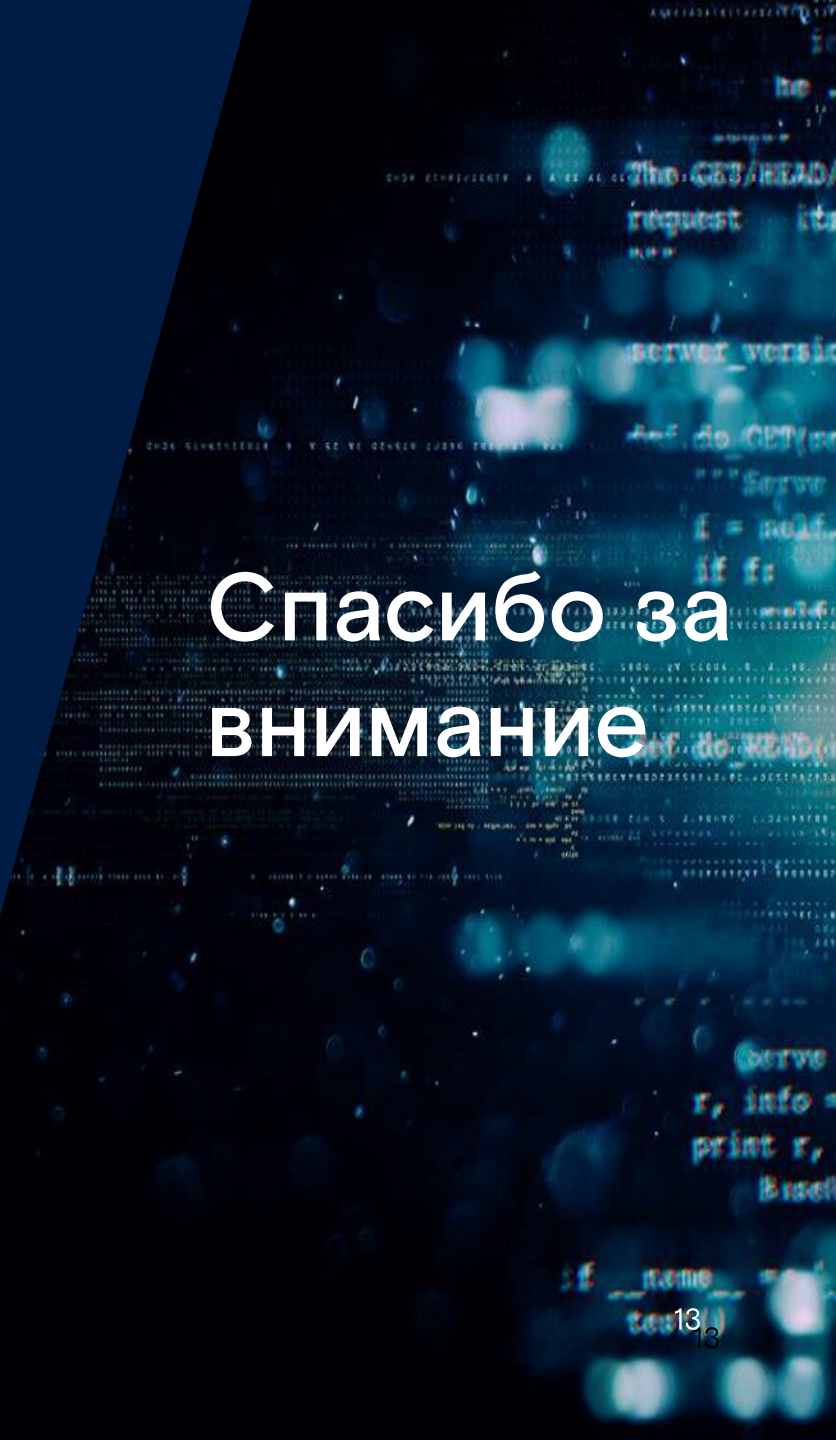
Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru

Ростелеком
Солар



13