"Безопасность IoT: чем выше ожидания - тем больше вопросов"

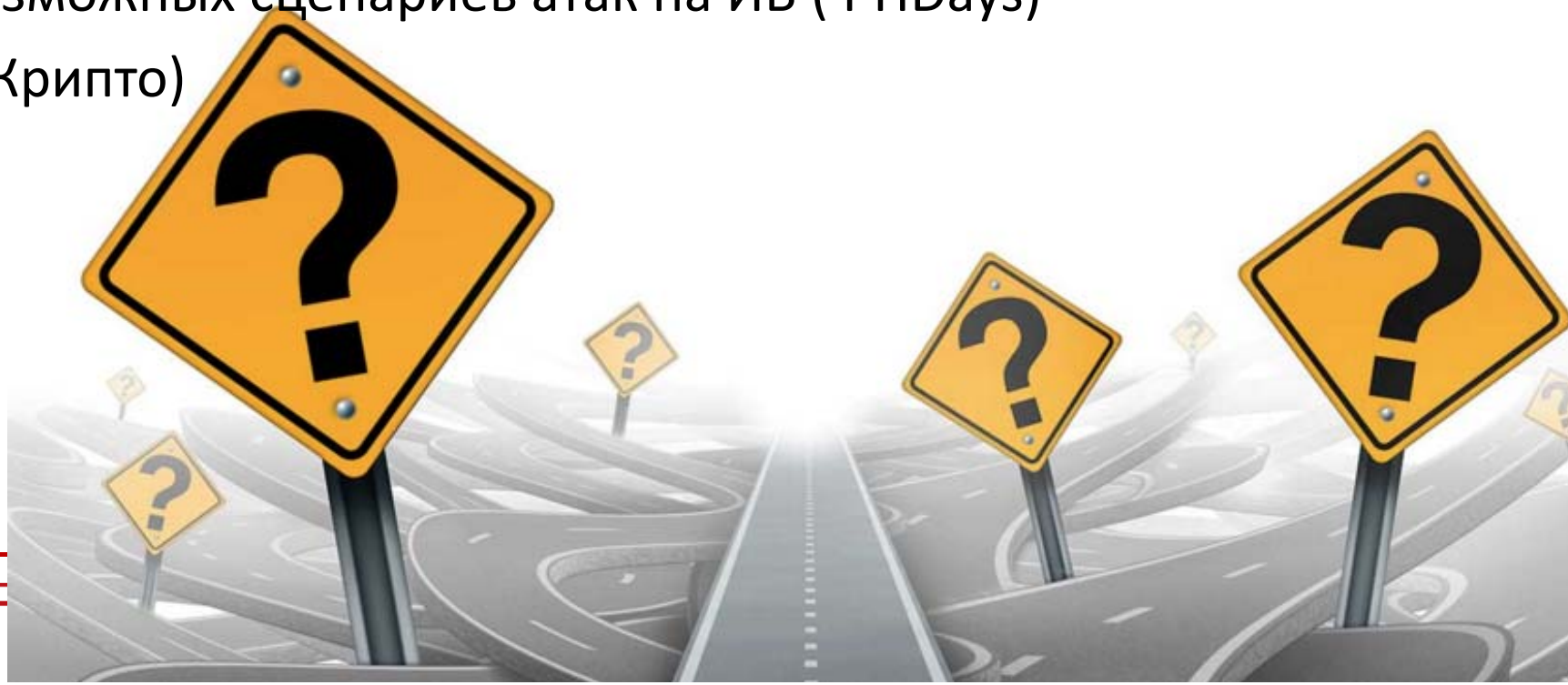
POSITIVE TECHNOLOGIES

Качалин А.И.

ptsecurity.com

Безопасность ИВ – интересная тема

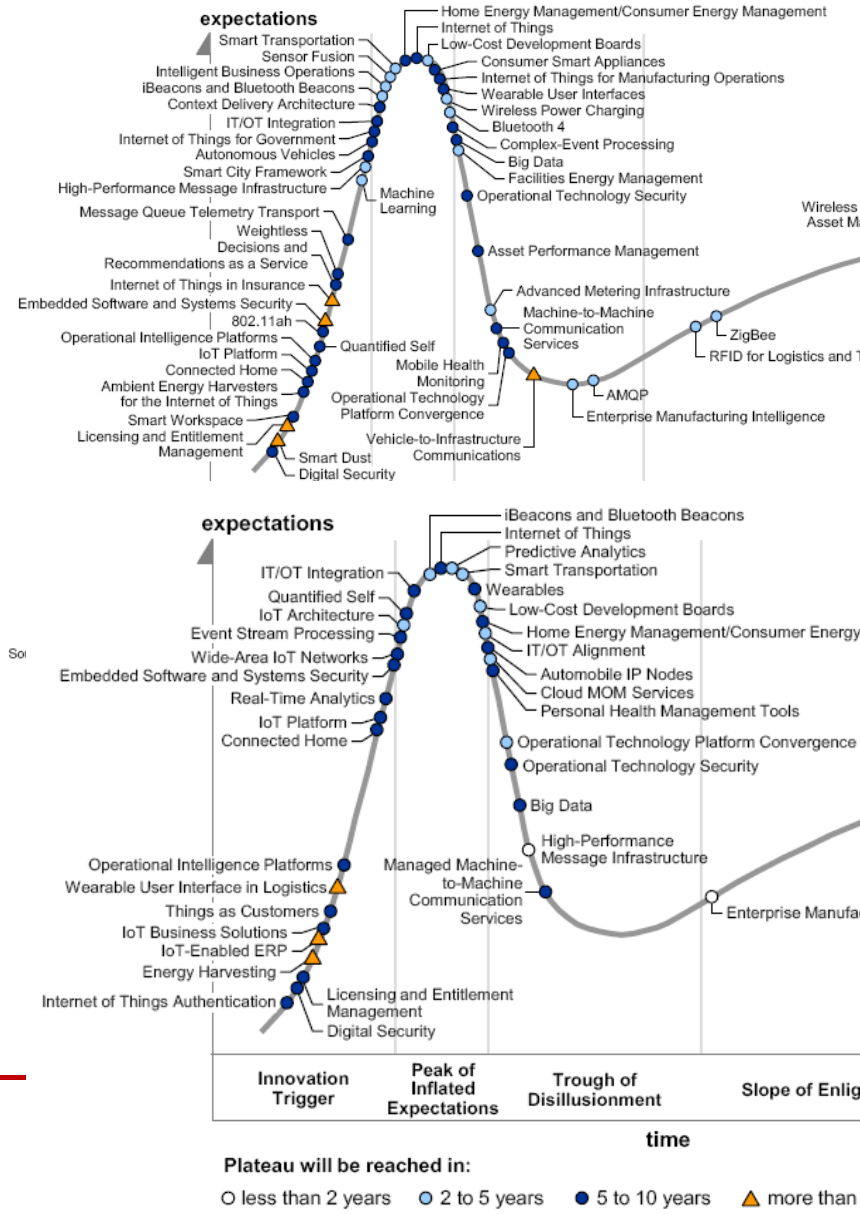
- Моделирование атак на автомобильную бортовую сеть и дорожную инфраструктуру
- Анализ угроз ИВ (РусКрипто)
- Прогноз возможных сценариев атак на ИВ (PHDays)
- ИБ ИВ (РусКрипто)



ИВ – что есть, что будет?

- Взрывной рост «объемов»
  - 6,5 миллиардов устройств в 2016 (+30% за год)
  - 21 миллиард устройств в 2020
- Прогнозируемость технологического развития?
- Интеграция в существующие ИТ
  - Концепция «Операционных Технологий»
- Рост и эволюция (параллельно с ростом объемов)
  - Развитие экосистемы и стандартов
  - Новые бизнес-модели – потребность в новых типах устройств, высокая динамика

Figure 3. Hype Cycle for the Internet of Things, 2014



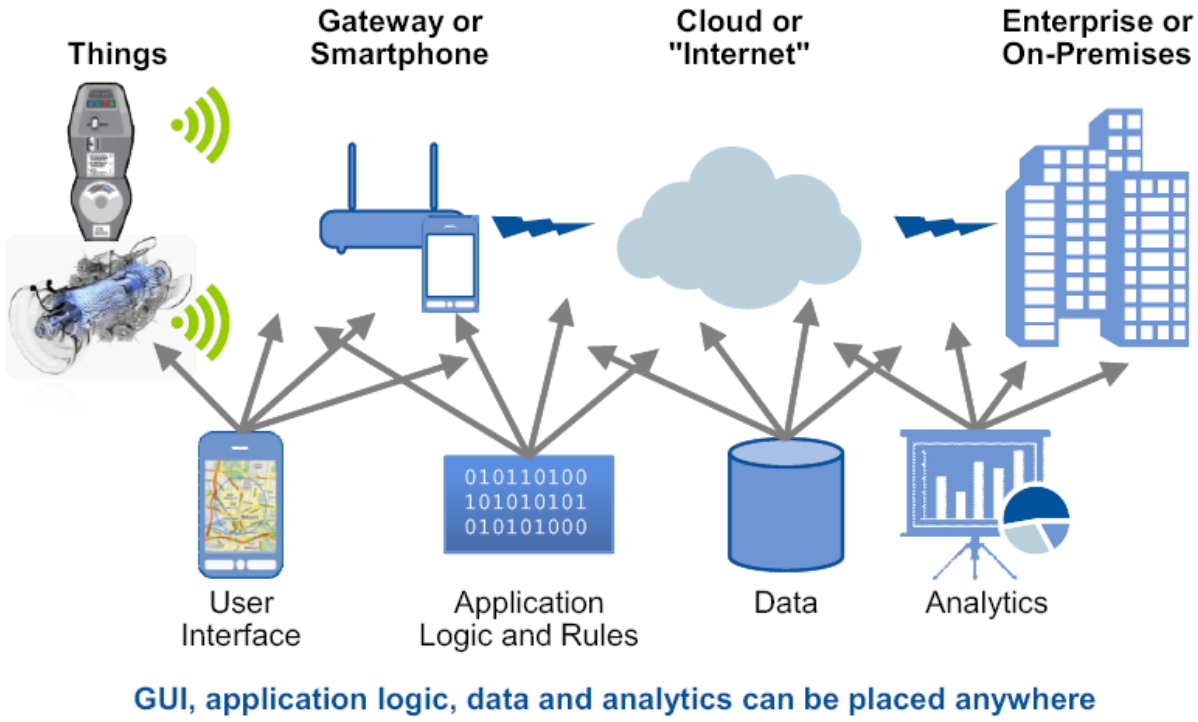
(Без)опасная архитектура ИВ

Как может быть построена и проанализирована модель угроз с учетом ИВ?

Точки рассмотрение ИБ:

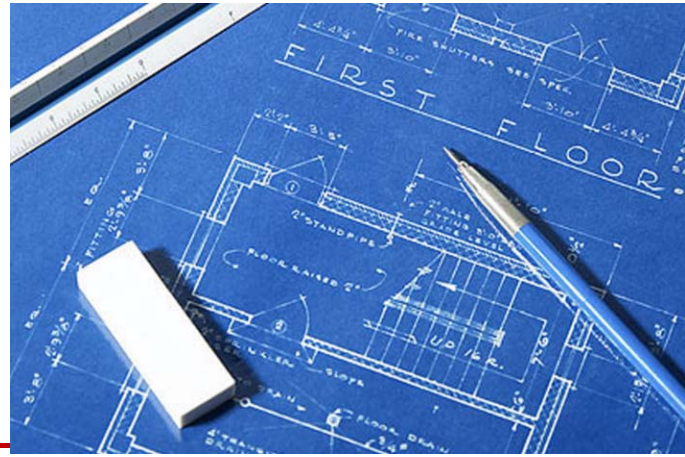
- С т.з. «вещей»
- С т.з. ИВ-шлюзов
  - Маршрутизаторов
  - Смартфонов
- С т.з. Облака?
- С т.з. Корпоративного сегмента

Figure 1. High-Level Architecture for the IoT



Архитектурные проблемы ИВ

- Метаданные
- Объем хранилища и место хранения данных
- Форматы и структуры хранения данных – соответствующие задачам
- Процедуры внесения и обработки данных превносимых устройств
- Гибкие процедуры интеграции и трансформации данных
- Требование к качеству данных: доверие и контроль
- Конфиденциальность данных
- Масштабируемость, эластичность
- Физическая распределенность и перемещение устройств



Типы устройств ИВ: «палка о более чем двух концах»

- Функциональность устройств ИВ
  - Класс 1: Простые сенсоры, приводы
  - Класс 2: с возможностью хранения и первичного анализа данных
  - Класс 3: Сложные устройства (близки к полноценным серверам)
- По возможности взаимодействия с физическим миром
  - Устройства сбора данных (сенсоры)
  - Устройства воздействия (приводы)
  - Устройства вывода данных (дисплеи)
  - Устройства, совмещающие функции сбора и вывод данных

ИБ-Прогноз погоды: весна ИВ

- Ещё более* ускоренные и небезопасные практики разработки
- Дополнительные* сложности в обновлении
- Меньшая* видимость аномалий для пользователя
- Больше* объектов защиты/для атаки

Временн**о**е окно уязвимости –
в 1,5-2 раза больше

* По сравнению ~~с тем как плохо сейчас~~ «классическим» ИТ

Безопасность ИВ – как 20 лет назад в «большом ИТ»

- Сеть
- Приложения
- Мобильные устройства
- Облака

\+ ----------

ИВ

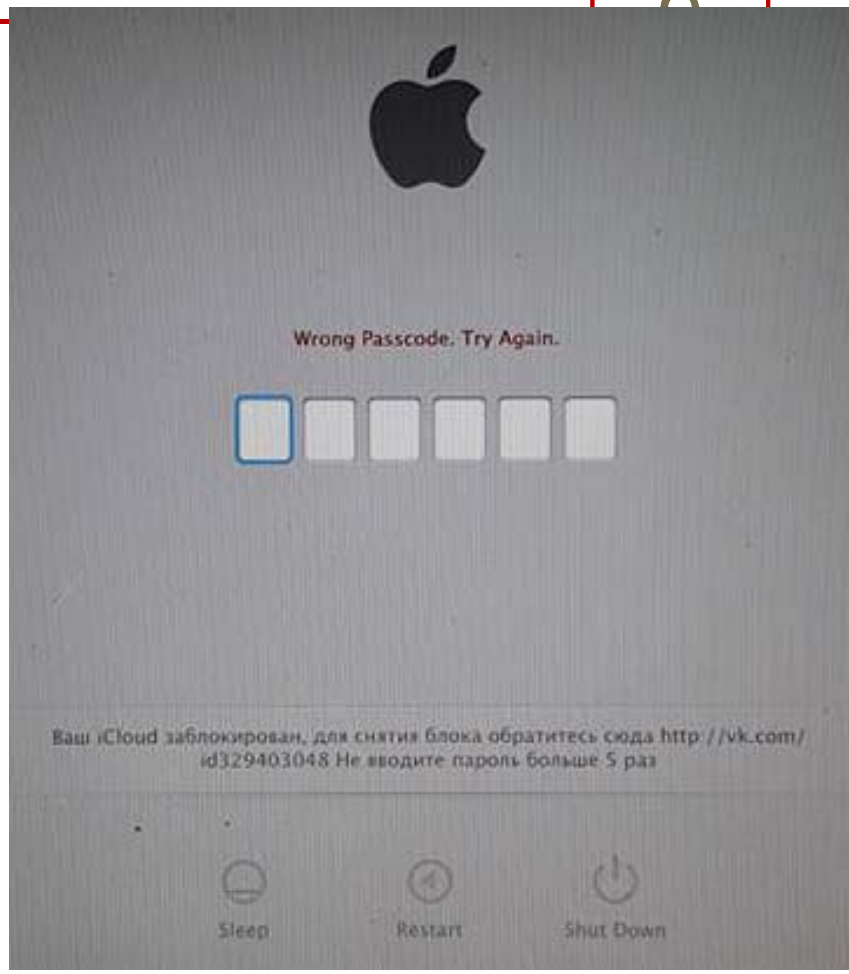
Примеры ИБ неуспехов ИВ

- 10/10 security systems accept ‘123456’
- 10/10 security systems with no lockout
- 10/10 security systems with enumeration
- SSH listeners with root/“” access
- 6/10 web interfaces with XSS/SQLi
- 70% of devices not using encryption
- 8/10 collected personal information
- 9/10 had no two-factor options
- Unauthenticated video streaming
- Completely flawed software update systems

https://www.rsaconference.com

ИВолюция атак

- Атаки на процедуры работы экосистемы: процедура утраты контроля над устройством и блокирование акаунта
- Открытость физическому доступу: сброс в небезопасное состояние
- «Вещь посередине»: не только прослушивание, но и «выполнение действий»
- Запрет ухода в ждущий (энергосберегающий) режим



Поверхности атак ИВ

- Экосистема
- Обмены в экосистеме
- Память устройства
- Физические интерфейсы
- Веб-интерфейсы
- Прошивка
- Сетевые сервисы
- Интерфейс администратора
- Локальное хранилище данных
- Веб-интерфейс доступа к облаку
- Интерфейс подключения сторонних компонентов
- Механизмы обновления
- Мобильное приложение
- API доступа вендора
- Сетевой трафик
- Аутентификация/Авторизация
- Конфиденциальность/приватность
- Аппаратные манипуляции(сенсоры)

OWASP Internet of Things (IoT) Project

ТОП10 угроз в ИВ?

OWASP Internet of Things (IoT) Proje

Top 10 IoT Vulnerabilities (2014) Project

The OWASP Top 10 IoT Vulnerabilties are as follows:

Rank	Title
I1 •	Insecure Web Interface
I2 •	Insufficient Authentication/Authorization
I3 •	Insecure Network Services
I4 •	Lack of Transport Encryption/Integrity Verification
I5 •	Privacy Concerns
I6 •	Insecure Cloud Interface
I7 •	Insecure Mobile Interface
I8 •	Insufficient Security Configurability
I9 •	Insecure Software/Firmware
I10 •	Poor Physical Security

Время ИВ: что ~~на~~ в твоих часах?

- Данные: почта, соц.сети, смс, звонки
- Информация о владельце: пульс, перемещения
- Возможность доступа
  - К мобильному устройству
  - В Интернет (WiFi) и учетные данные
- Прошивка и приложения
  - Данные приложений
- Средства аудио-, видео- записи

А что авто? Гонка продолжается

- ✓Прогнозируемые угрозы: атаки на бортовую сеть (мультимедиа) и взаимодействие с дорожной инфраструктурой
- ✓Превентивные меры: невозможность доступа к контуру управления
- ✓Развитие и усложнение бортовой сети автомобиля
- ✓Демонстрация возможности полного контроля над бортовой сетью автомобиля через технологическое подключение
- ✓Демонстрация возможности удаленного доступа для управления мультимедиа и функциями управления
  - ✓Запрет входящего трафика
  - ✓Отзыв 1млн автомобилей на обновление программных и аппаратных компонентов
- ✓Демонстрация возможности исполнения кода через аудио-диск (уязвимость в проигрывателе)
  - ✓Обход запрета входящего трафика

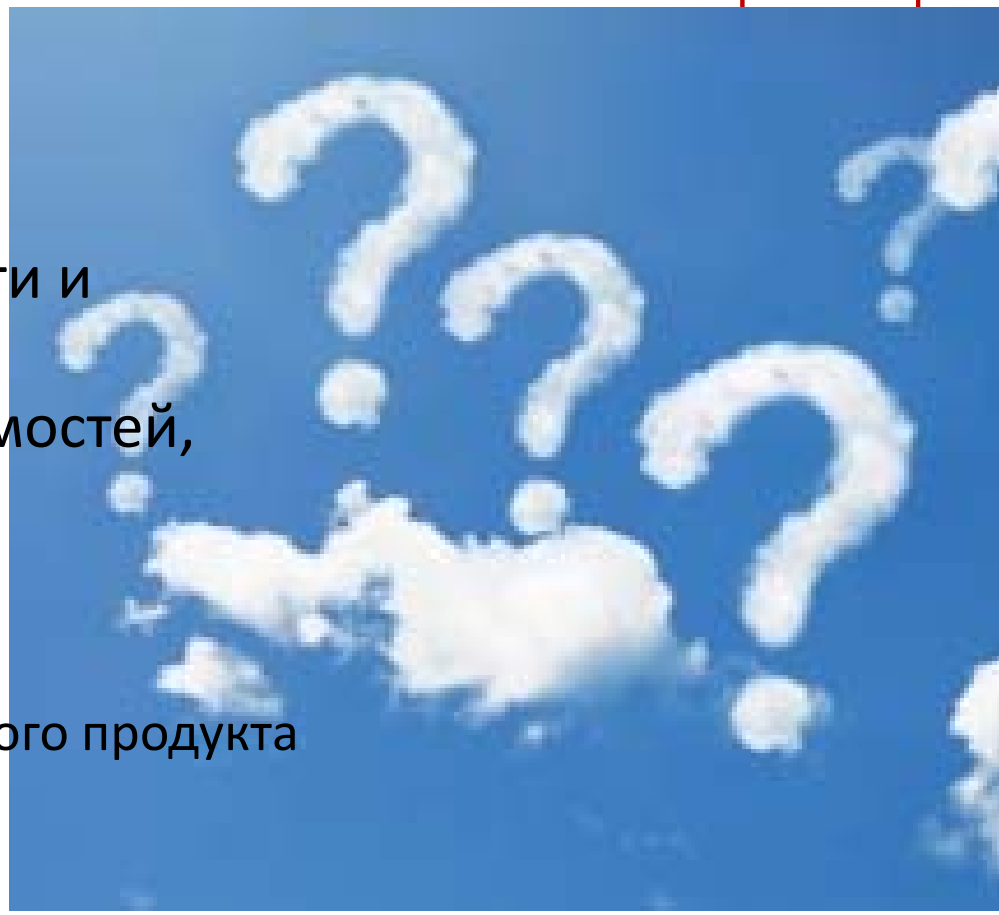
Зачем угонять один автомобиль, если можно угнать целый корабль автомобилей?

- Изменение всех характеристик корабля: позиция, груз, название
- Создание несуществующих кораблей: «иранский корабль с ядерным грузом у берегов США»
- Создание подложных навигационных объектов (буйков, маяков)
- Задание ложных регионов спасательных операций
- Вброс ситуации «человек за бортом» - тревога в радиусе 50км
- Подложный прогноз погоды

HITB Con: DR. MARCO BALDUZZI, KYLE WILHOIT, ALESSANDRO PASTA:
Hey Captain, Where's Your Ship? Attacking Vessel Tracking Systems for Fun and Profit

Открытые вопросы ИБ ИВ

- Бурное развитие технологий
- Проблемы совокупности технологий
  - Возвращение старых проблем
- Проблемы масштабов, разнородности и мобильности устройств
- Неизвестный ландшафт угроз, уязвимостей, атак
- Проблематичность
- Скорость разработки решений ИВ
  - Проклятие минимально-жизнеспособного продукта (MVP)



Спасибо!

Алексей Качалин akachalin@ptsecurity.com

POSITIVE TECHNOLOGIES

ptsecurity.com