Вопросы безопасности IoT: проблемы и решения

Дмитрий Белявский, ТЦИ

Киберсекьюритифорум-2017
Москва, 3 февраля 2017 г.

Что такое IoT?

- **Устройства, способные объединяться в сеть**
- **Разнообразные аппаратные возможности**
  - Процессоры: от RFID до ARM
    - От 10 мГц до 2 ГГц
  - Память: от 2 кб до 1Гб

Ограничения устройства

- Ограничения по цене
- Ограничения по питанию
- Жизненный цикл
- Обновление Firmware
- Датчик случайных чисел
- Трудности программирования

Представление о безопасности

- «WEP кажется образцом дизайна»
- «Атаки как в 1990-х»
- 250 стандартов по IoT, из них только 5 – по защите информации (Алексей Лукацкий на РусКрипто-2016)
- IETF слабо задействован в процессе

- **Буква S в аббревиатуре IoT обозначает Security.**

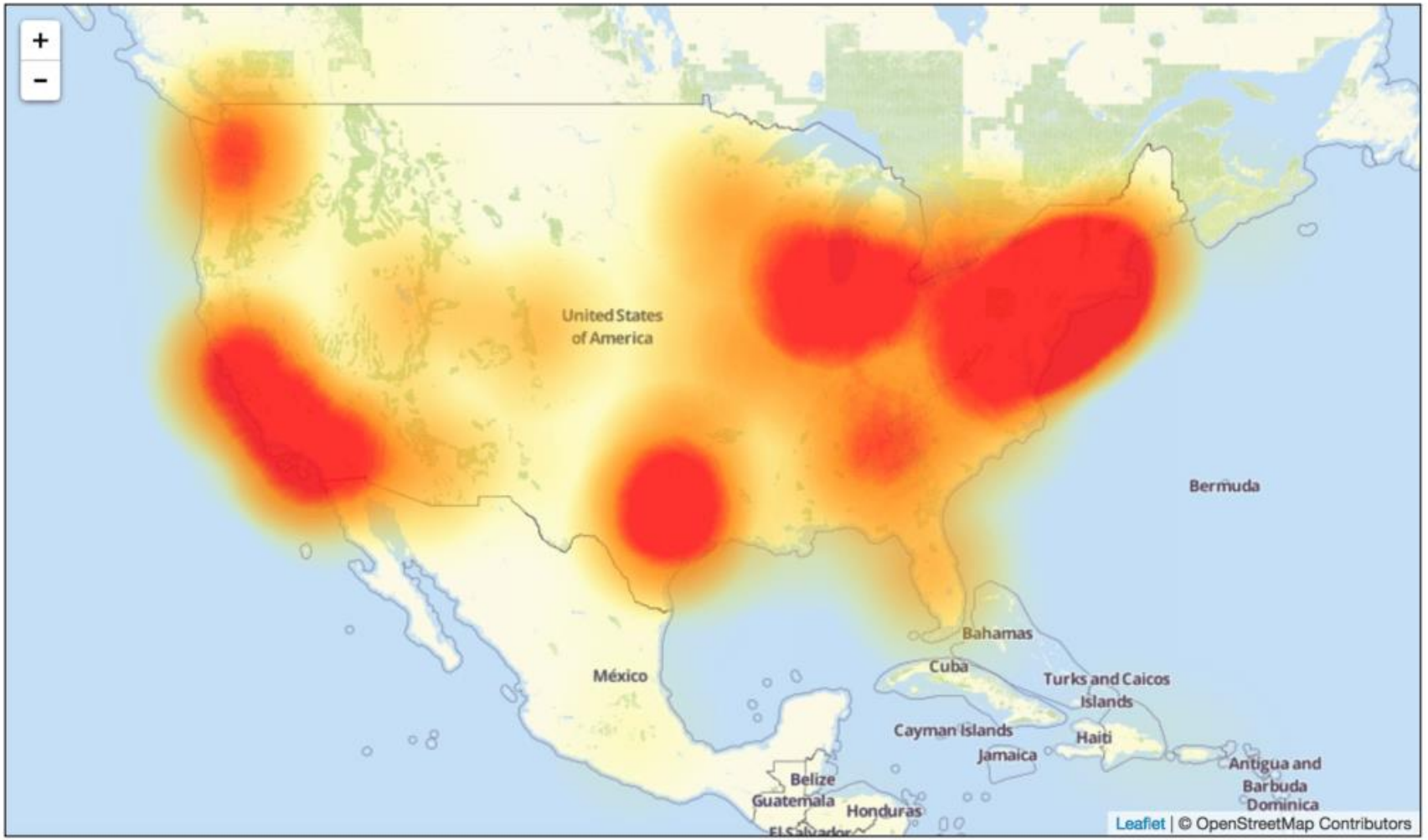
Свежая хроника

- **ZyXEL**
  - роутеры, реквизиты администратора
- **Samsung**
  - SmartCam, выполнение произвольного кода
- **NETGEAR**
  - сетевое оборудование, обход авторизации
- **Cisco**
  - Prime Home, обход авторизации

Атака на Dyn

- **21 октября 2016 года**
- **Несколько волн атаки**
- **DDoS с применением ботнета Mirai**
  - Роутеры, видеокамеры, DVR…
- **Сколько**
  - До 1,2 терабит/с
- **Последствия**
  - Нет доступа к Twitter, Amazon, Tumblr, Reddit, Spotify, Netflix.

Карта «на пике»



Удобство пользователя

- **Массовый рынок**
  - Простота, простота, простота!
- **Реквизиты доступа по умолчанию**
  - Иногда – без возможности изменить
- **Последствия: DDoS-атаки**
  - Crebsonsecurity.com, Dyn, OVH
- **Mirai: ботнет-«миллионер»**
  - До 1,5 терабит/с на пике

Open Source

- **Урезанный Linux**
  - От внесения ошибки до исправления – несколько лет
- **Баги в утилитах => баги в прошивках**
  - Heartbleed: найден в 2014 году
  - 200000 уязвимых устройств на начало 2017 года

Что делать: разработка

- **Инициализация**
  - https://tools.ietf.org/html/draft-sarikaya-t2trg-sbootstrapping-03
- **Сценарии обновления**
  - https://tools.ietf.org/html/draft-farrell-iotsu-workshop-00

Что делать: бизнес

Вопросы к вендору

- Сколько лет поддержки?
- Как меня оповестят об изменениях?
- Есть ли отчёт о security-тестировании?
- Как сообщать о найденных уязвимостях?
- Используется ли криптография?

Что делать: государство

- **FTC: конкурс с призом на 25000$**
  - Защита от старых уязвимостей
- **Автомобили**
- **Кардиостимуляторы**
- **Промышленная безопасность**
- **Бытовая техника**
- **Усилий одной страны не хватит**

Не только IoT

- **Никто не меняет настройки**
  - http://www.theregister.co.uk/2017/01/11/wireless_router_insecurity_survey/
- **FTP-серверы – хостинг для Malware**
- **Внутренние сервисы на внешних адресах**
  - Hadoop, MongoDB…

Что в России?

ТК 098 Росстандарта

- «Интернет вещей» (Internet of things)
- «Умные города» (Smart cities)
- «Большие данные» (Big data)
- «Умное производство» (Smart manufacturing)

Q&A

Вопросы?

beldmit@tcinet.ru