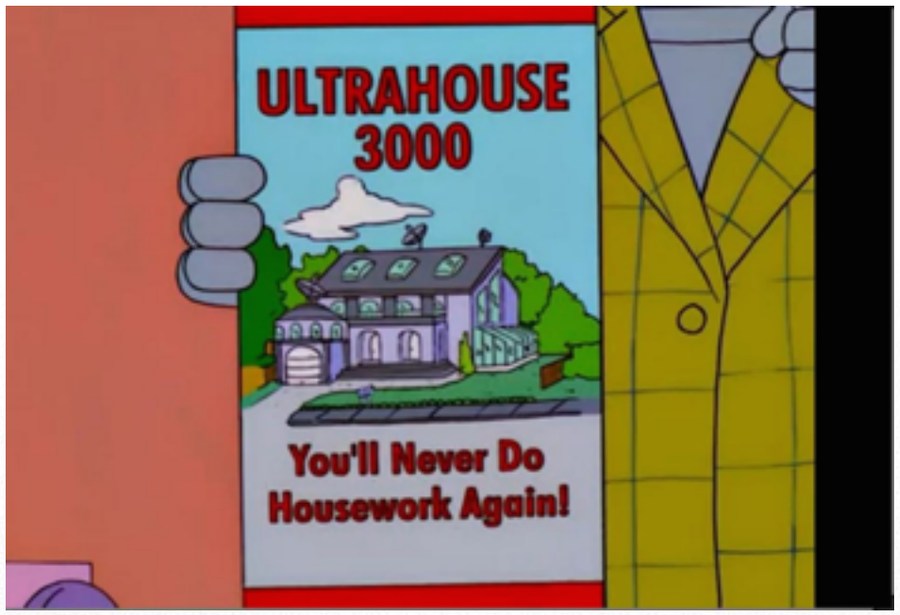
# Армия освобождения домохозяек: структура, состав вооружений, методы коммуникации

Петухов Андрей

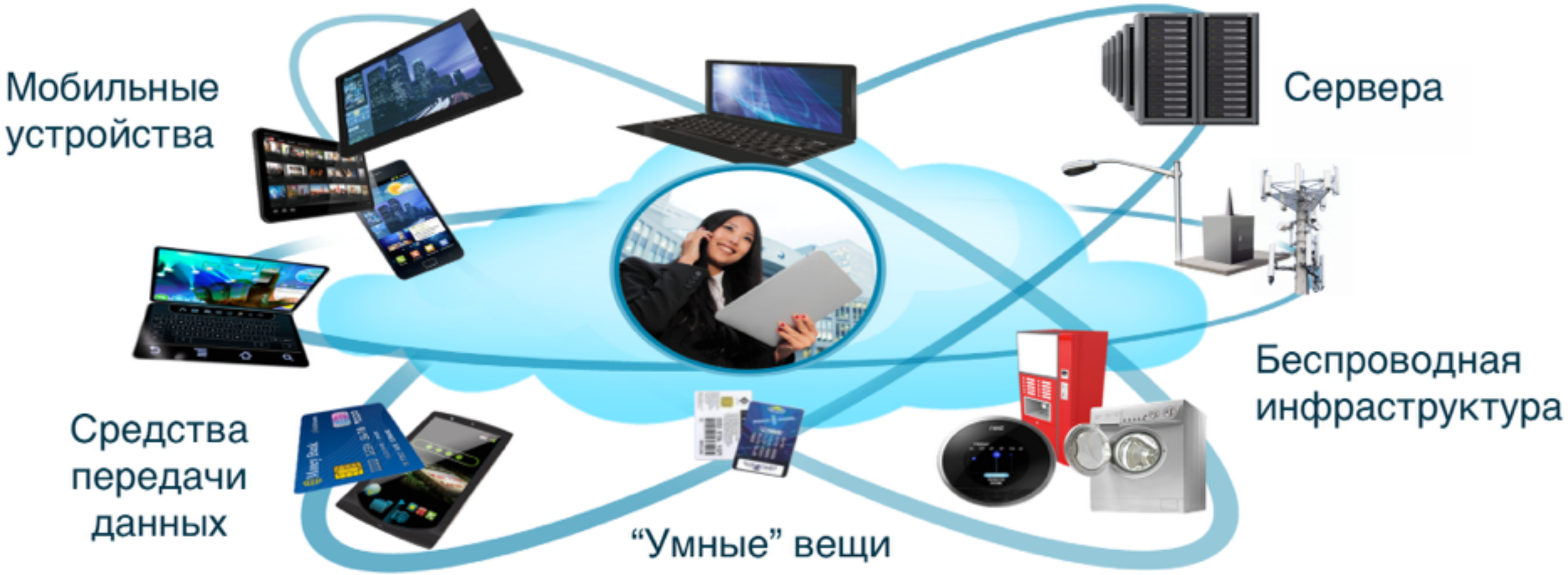
ЛБИС ВМК МГУ

РусКрипто 2014

# Бытовое представление IoT




# Технологическое представление IoT



# Примеры из IoT

- Умный дом
  - ➡ сигнализация (о ворах, о пожаре, о протечках), освещение, климат-контроль, управление разморозкой продуктов, ТВ и медиа-системы, IP-камеры, унитаз, irobot, приставки (в т.ч. kinect)
- Умные сети электроснабжения
- Пассивные метки (RFID) в логистике, инвентаризации, предотвращении краж, платежах, изучении миграции животных, системах контроля доступа (в т.ч. паспортах)
- Сети из активных элементов в задаче получения данных об окружающей среде (smartdust)

# Технологии IoT, подробнее

- Средства идентификации и считывания
  - RFID, NFC, QR, штрих-коды и т.д.
- Средства измерения
  - сенсорные сети
- Средства передачи данных
  - IEEE 802.15.4 (Phys / MAC), ZigBee, WirelessHart, MiWi, 6LoWPAN, PLC
- Основа для умных вещей
  - ARM, дистрибутивы Linux для встроенных систем

# Nothing Ever Changes или откуда берутся уязвимости

- Зачем изобретать велосипед, возьмем существующие дистрибутивы и допилим их под себя!
  - известные уязвимости в стандартном ПО
  - ненужные компоненты, предоставляющие интерфейс вовне
  - “security hardening”? Ой, а что это?
- Давайте изобретем свой протокол, свою ОС, свой веб-сервер и напишем свой софт!
  - собственные уязвимости в коде
- Для управления устройством, сделаем удобный интерфейс через HTTP/Bluetooth, а в руководстве обязательно напишем про пароли
  - пароли по умолчанию, настройки по умолчанию
- К.О.: недостатки появляются в областях ответственности тех участников жизненного цикла устройства, где про ИБ мало знают

# Итого

- Использование стандартного ПО с уязвимостями
- Ошибки в собственном коде (обычно веб-компоненты)
  - ошибки авторизации, CSRF, OS command injection, и т.п.
- Небезопасные настройки используемых компонент
  - пример: unauthenticated UPnP
- Слабая защита от исследования и обратной инженерии
  - всплывают “сервисные” учетные записи
  - находится несложный обход доверенной загрузки ОС
- Небезопасная эксплуатация
  - пароли по умолчанию
  - словарные пароли
  - отказ от обновлений
  - подключение к Интернет напрямую (например, через PLC или 3G)

# Посмотрим на это строже

- В стандартном варианте умные устройства подключены к домашней сети или управляются по Bluetooth/ИК
  - ➡ активное воздействие из Интернет на них невозможно
- Остаются нарушители класса “человек рядом с домом” и “человек за периметром”
- “Человек рядом с домом” - есть ли мотив?
  - ➡ исследования? - не страшно
  - ➡ хулиганство? - тоже не очень с точки зрения последствий
  - ➡ таргетированная атака? - возможно, для слежки
- “Человек за периметром” - как он туда попал и каков был мотив?
  - ➡ ИК и bluetooth устройства не пострадают
  - ➡ захвачен компьютер/телефон, атака таргетированная - логично, слежка
  - ➡ захвачен компьютер/телефон/маршрутизатор, атака нетаргетированная - развитие атаки на окружение через autopwn - пока не видел, но выглядит не нереально!

# Выводы для “домохозяйки”

- [Безысходность] Если моссад захочет провести целевую атаку, он ее проведет в любом случае
- [Надежда] Маршрутизатор на периметре - Минас Тирит вашего свободного западного мира умных вещей
- [First things first] Если у вас может быть захвачен маршрутизатор на периметре, то бояться стоит в первую очередь за свои данные (в т.ч. учетные), а не за армию умных вещей

# Вопросы???


- Twitter: @p3tand
- Email: petand@seclab.cs.msu.su