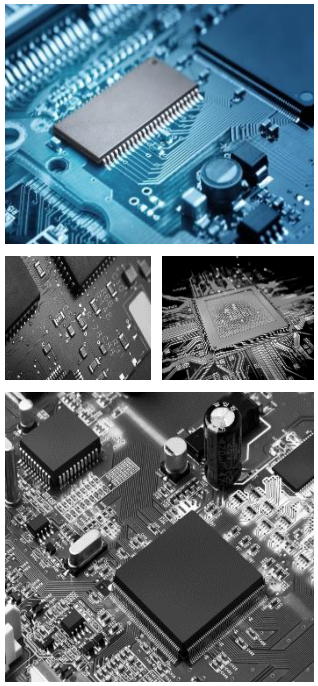
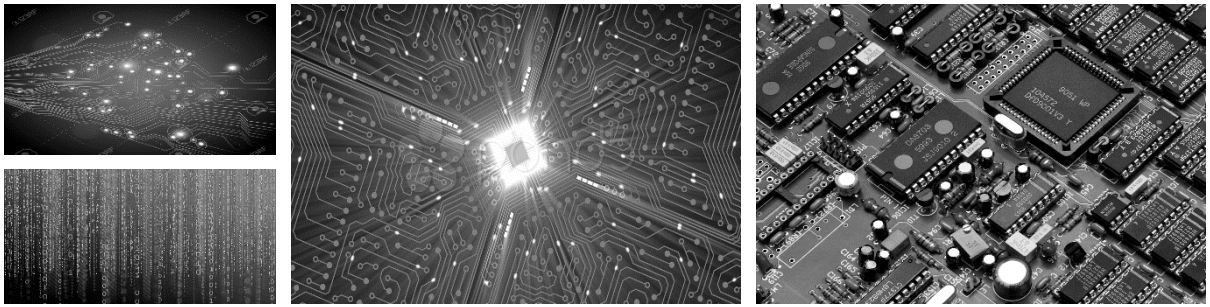




Вопросы безопасности сетевой инфраструктуры IoT

г. Москва,
21 февраля 2017 г.

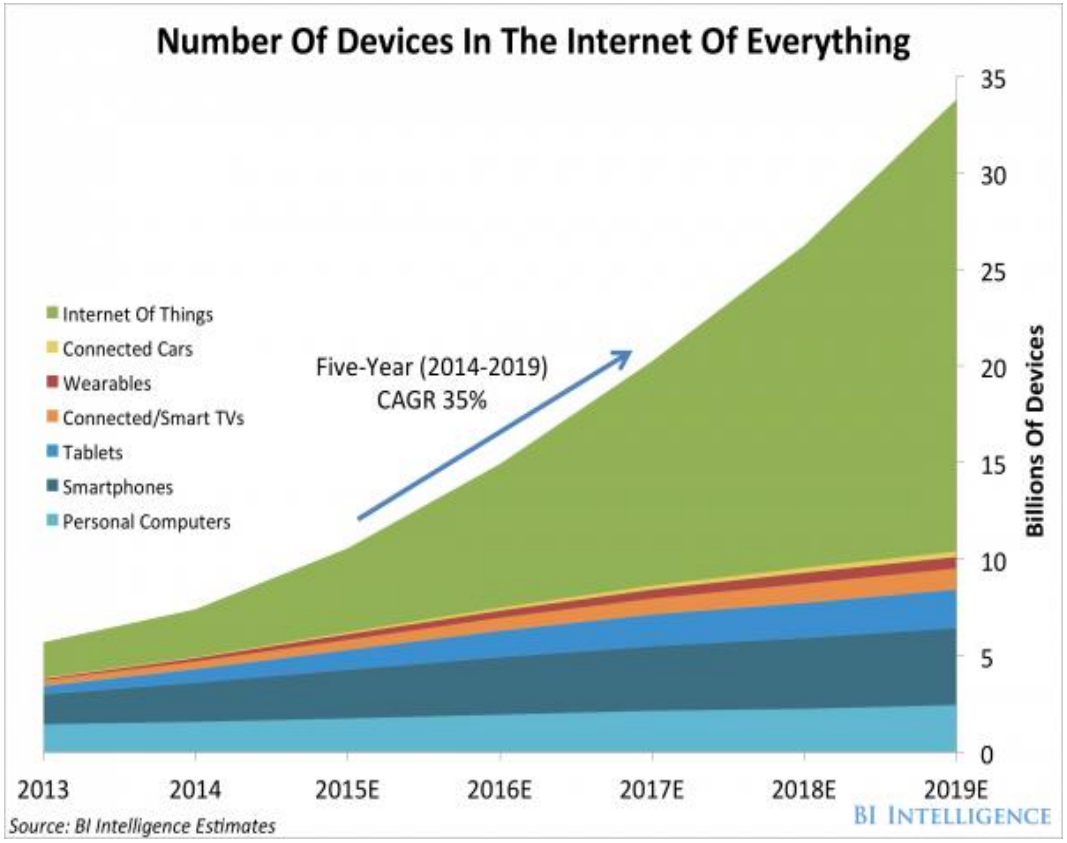
Борис Кривошеин
Исполнительный директор ООО «ИнЧип Технологии»

Тенденции развития

К 2020 г. – от 15 до 50 млрд. IoT устройств

Сферы массового применения:

- Промышленность – «Индустрия 4.0»
- Транспорт – мониторинг и управление движением, автоматизация ТС
- Энергетика – системы управления энергопотреблением
- Медицина – контроль состояния пациентов 24/7
- Городская среда обитания - «Умные» здания, районы, города



Угрозы безопасности в эпоху IoT

Факты:

- Взрывной рост «поверхности проникновения угроз» и мощности сетевых атак
- Создание botnet-сетей из сотен тысяч и миллионов IoT устройств

DDOS атаки на провайдера Dyn и др. в сентябре-октябре 2016:

- Botnet Mirai –от 600 Гбит/с до 1 Тбит/с, 150 тыс. IoT устройств

DDOS атаки на российские банки в октябре-ноябре 2016:

- Botnet под контролем 1 человека (>24 тыс. IoT устройств, продолжительность атаки - 12 часов).

DDOSaaS:

- Стоимость услуг – от $5 в час.

Слабость защиты IoT устройств

- Ограничения производительности и объёма памяти IoT устройств, не позволяющие использовать «полные» сценарии сетевой защиты
- Использование предустановленных паролей (более 60% частных и около 20% корпоративных пользователей не меняют их)
- Производители IoT оборудования заботятся в первую очередь о функциональности и стоимости, безопасность реализуется по остаточному принципу
- Неконтролируемые процессы разработки и производства IoT устройств, возможность внедрения различных «закладок» в цепочке поставки
- Ограниченные возможности по обновлению прошивок в случае обнаружения уязвимостей
- Новые протоколы и сценарии сетевого взаимодействия IoT, ограничивающие возможности мониторинга

- **Невозможность применения традиционных методов защиты на стороне клиента (антивирусы, программные шлюзы, настройки политик безопасности и т.п.).**

Методы противодействия

На этапе разработки

- Защита интерфейса управления
- Авторизация (аутентификация) пользователей и встречного оборудования
- Ограничение доступности сетевых портов и служб
- Реализация криптозащиты на транспортном и канальном уровне
- Защита (шифрование) персональных данных, хранящихся в устройстве
- Ограничения в конфигурации устройства пользователем для гарантии минимально допустимого уровня защиты (стойкость паролей, длины ключей шифрования и т.п.)
- Возможность защищенного обновления и контроль целостности встроенного ПО
- Защита от взлома путём физического вмешательства

На этапе эксплуатации

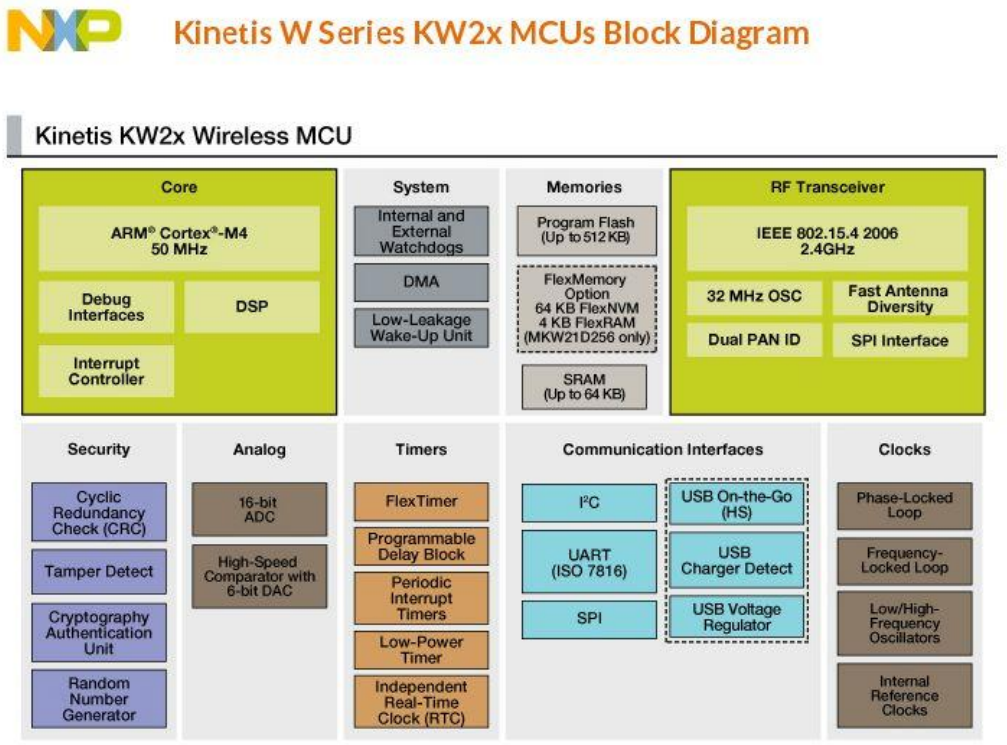
- Сегментация сети, изоляция либо разделение шлюзами IoT сегментов и критичных для безопасности сегментов сети
- Создание надёжных политик безопасности для IoT устройств

Технологии, необходимые для защиты

- Полная модель безопасности для сетей, включающих IoT шлюзы и IoT устройства
- Устройства для построения защищенной сетевой инфраструктуры
- Граничные маршрутизаторы с поддержкой защищенного стека протоколов (IEEE802.15.4 / 6LoWPAN / Thread …)
- Средства разработки, обеспечивающие базовые механизмы защиты
  - Kura (Eclipse Foundation)
  - ESF (Eurotech)
  - IAR Embedded Workbench (Silicon Labs)
- Технологии сбора и обработки больших массивов данных
  - NoSQL
- Средства мониторинга и управления сетями IoT

Современный уровень – IoT SoC NXP

Компоненты системы безопасности Kinetis KW2x:



Источник: NXP Corp., USA, 2016

- **Secure FLASH –** защита команд и данных от неавторизованного доступа
- **Крипто ускоритель–** поддержка алгоритмов DES, 3DES, AES, MDA, SHA
- **Радиомодуль –** поддержка стеков протоколов IEEE 802.15.4: Thread, ZigBee, 6LowPAN, WirelessHART, ISA 100.11a
- **Генератор случайных чисел –** по требованиями FIPS 140
- **Блок защиты от физического взлома –** очистка памяти, сброс системы

Основные векторы развития и базовые элементы IoT

- **Высокая степень интеграции:** реализация всех основных требований по назначению в одной системе на кристалле
- **Процессорные ядра:** высокая пиковая производительность в совокупности с энергоэффективностью, возможность работы в «импульсных» режимах
- **Радиотракт:** независимая подсистема с аппаратной поддержкой протоколов IoT и функций обработки пакетов
- **Защита информации:** аппартные ускорители криптографических функций, блоки защиты от НСД и реинжиниринга с учётом неограниченного физического доступа к системе
- **Гармонизация:** совместимость с международными и национальными стандартами и регламентами в сфере IoT

Завоевание рынка IoT

Объединение усилий :

- Создание базовых доверенных технологий IoT, доступных широкому кругу отечественных разработчиков;
- Создание экосистемы отечественных компаний-разработчиков, интегрированной в мировой рынок IoT.

Результаты:

- Технологическая независимость отечественных IoT систем;
- Защита информационных систем, внедрение доверенных IoT решений на современном техническом уровне.

Цели и задачи

Разработка СФ–блоков

- Крипто ускорители – поддержка ГОСТ 34.12-2015 («Магма», «Кузнечик»)
- Радиомодули – аппаратная поддержка стеков протоколов IEEE 802.15.4, открытая архитектура
- Встроенная память с защитой данных, защита от физического взлома

Разработка IoT систем на кристалле

- Открытая нелицензируемая архитектура
- Специализированная ОС IoT отечественной разработки
- Конкурентная цена

Разработка IoT устройств массового потребления

- Отечественная ЭКБ
- Технологически независимые средства разработки IoT решений
- Средства внедрения и обслуживания безопасных гетерогенных сетей с поддержкой IoT устройств
- Рост внутренних компетенций российских компаний в отрасли IoT

Контакты

ООО «ИнЧип Технологии»
Россия
105005 Москва
ул. Радио 24 к.1
T +7 499 281 65 63
E contact@inchip.tech
http://www.inchip.tech