Проблемы доверия к импортной электронике на базе SoC (System-On-Chip)

- Особенности построения систем на базе SoC
- Архитектура современных ARM-процессоров, проблема закладок в процессорах
- Что такое TrustZone и для чего сделана
- Насколько эффективна сертификация ОС и приложений?
- О возможности "стерилизации" зарубежных ARM-процессоров и создании доверенной аппаратно-программной среды

Сергей Груздев
Ген. директор
Аладдин Р.Д.

Проблема "последней мили" - немного фактов

- Взлом экранов (систем оповещения) в публичных местах становится регулярным
- 13 августа 2013 г., дворец Республики в Алматы
  - Несколько часов крутилась порнушка
  - Организовал хакер со своего мобильного телефона
- 3 августа 2010 г., Парламент Индонезии
  - На экране, отражающем ход голосований, полчаса крутилась порнушка
- 18 марта 2009 г., Нью-Йорк
  - Взломаны электронные дорожные знаки
  - По всему городу транслируется сообщение "Нью-Йорк гибнет"
  - Это привело к массовым авариям, панике и гибели людей
- Январь 2009 г., Москва
  - Показ порнофильма на больших экранах на Садовом кольце
  - Глухая пробка, сбой в работе наземного транспорта
- 13 февраля 2013 г., США
  - Взломана вся система эл. оповещения населения
  - Трансляция "сцен ужасов" и сообщений о нападениях зомби

Проблема "последней мили" - немного фактов

- Ложные оповещения
  - 4 июля 2011 года, в День независимости США - сообщение об убийстве Б. Обамы
  - Май 2012, Китай - сообщение о приближающемся землятресении
  - Июнь 2007 - сообщение о ядерном взрыве в Чехии с трансляцией "картинки с места события" (50,000 человек сорвались со своих мест)
- Проблема в уязвимости конечного оборудования и возможности перехвата управления
  - IP-камеры
  - Плейеры контента для экранов
  - Исполнительные устройства
- Проблемы при расследовании произошедших инцидентов
  - Подмена контента в архивах
  - Ответственность - кто давал команды? Какие? Что транслировали или получали с камер?

Нужна доверенная платформа, работающая с доверенным контентом

Но всё это лишь детские шалости…

На чём построена современная электроника

- Большинство современных устройств построено на базе микропроцессоров архитектуры ARM (System-on-Chip - SoC)
  - Мобильные телефоны, планшеты, эл. книги
  - Smart-TV, TV-приставки
  - Интеллектуальные платёжные терминалы (POS, ATM)
  - Медицинское оборудование, принтеры, копиры
  - Автомобильная и бортовая встраиваемая электроника (мультимедиа-навигация-связь)
  - Промышленная автоматика (в АСУ ТП, контроллеры)

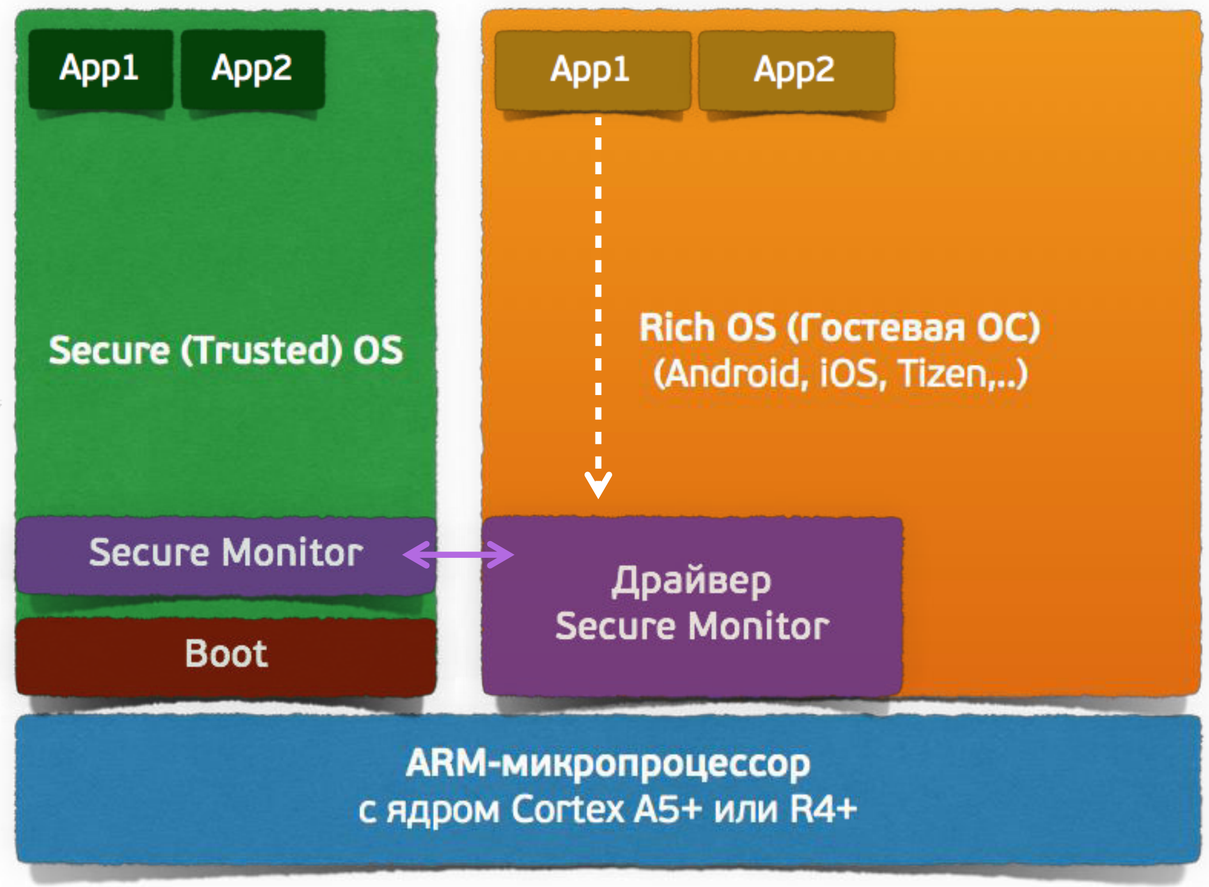
На чём построена современная электроника

- Начиная с ARM Cortex A5 (мультимедийные процессоры) и R4 (для промышленной электроники и встраиваемых систем), в микропроцессорах появилась т.н. TrustZone
  - TrustZone - аппаратная изоляция (виртуализация) двух параллельных процессов ("миров")
    - "Доверенного" / безопасного (Secure World)
    - Нормального / обычного (Normal World), где работают приложения под управлением привычных ОС - Android, iOS, Linux, Tizen, Sailfish,..

Архитектура современного ARM-процессора

Управление обменом с периферией производится через TrustZone*

** - Если загружена Trusted OS*



#1 - Загрузчик

- получает управление сразу после включения питания, стартует Secure OS

#2 - Secure OS загружает "гостевую" RichOS

- получает управление сразу после включения питания

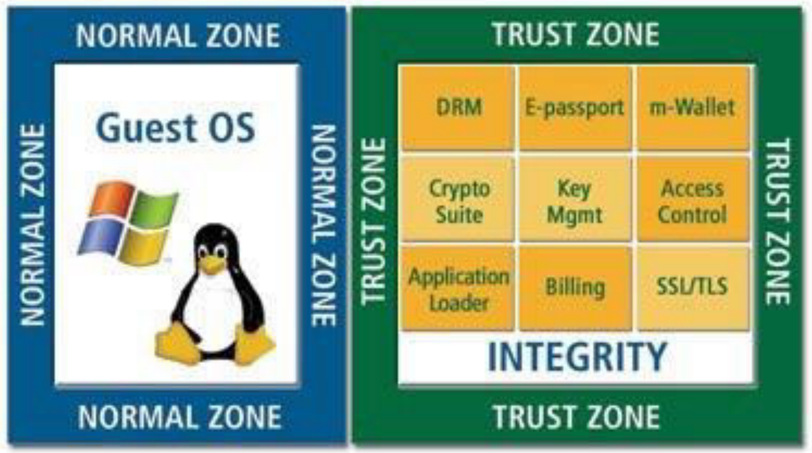
#3 - Secure OS может контролировать всё

- приложения и сама RichOS узнать об этом не могут

Кем и для чего сделана TrustZone

Кем?

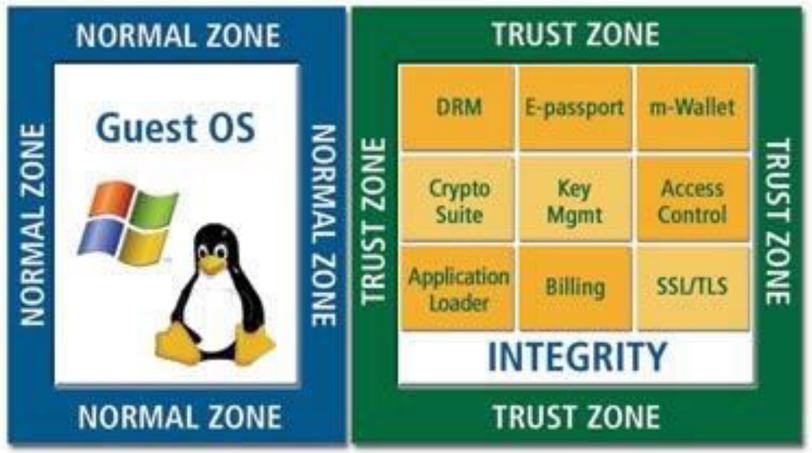
- Технология TrustZone была разработана английской компанией ARM и добавлена в архитектуру современных микропроцессоров SoC
- Технология была стандартизирована в 2010 г. и легла в основу Device GlobalPlatform
  - Для M2M, IoT в первую очередь



Кем и для чего сделана TrustZone

Для чего?

- Контроль за распространением контента (DRM)
  - Платное TV, музыка, видео (с защитой - привязывание лицензии к конкретному устройству)
- Безопасность платежей
  - Secure PIN (вводится из Secure OS, защищено от перехвата из "гостевой" ОС)
  - Безопасное хранение криптографических ключей (шифрования, подписи), выполнение криптоопераций в изолированной среде (Secure OS)
  - Безопасная визуализация данных (при подтверждении транзакции)
- Доверенные корпоративные приложения
  - Удалённый безопасный доступ, VPN, аутентификация
  - Защищённая почта
  - Защищённая передача данных, голоса
    - Пример: KNOX-2 (Samsung)



В чём проблема

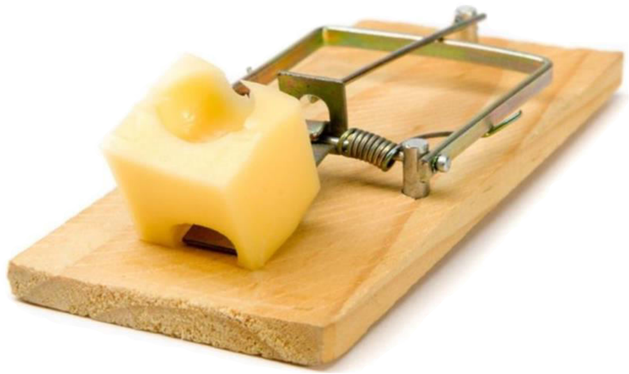
- Практически все крупные производители устройств на базе ARM-архитектуры стали выпускать свои устройства с "закрытой" TrustZone
  - Многих крупнейших производителей (Китай, Тайвань, Корея) купили* американцы (*проинвестировали*)
  - Они стали выпускать свои устройства на процессорах с "закрытой" TrustZone (с модулем от АНБ)
  - Многие из производителей пользуются Reference design (т.е. то, что им дали американские "инвесторы"), не понимая, что внутри
    - Инциденты на китайских биржах => падение курса юаня?

В чём проблема

- Приложение из TrustZone может скрытно (и необнаруживаемо) выполнять шпионские функции
  - Включать микрофон, камеру, вывод на экран, контролировать обмен данными, манипулировать информацией (подменять GPS/Глонасс координаты и пр.), красть криптографические ключи, отпечатки пальцев (с сенсора), ключи для доступа в гос. и корпоративные информационные системы и т.п.
  - В рамках страны возникают большие риски, что может быть "вырублена" связь и инфраструктура управления, полностью контролируются перемещение транспорта, людей, информационные потоки
  - Ряд стран уже озаботился проблемой использования процессоров с TrustZone, запретил их использование в критически важных системах и ведёт разработку собственной действительно доверенной Trusted OS

Даёт ли что-то сертификация ОС и приложений?

- Практически все современные ARM-процессоры содержат механизм TrustZone
  - Если она "закрыта" (а в 99% она "закрыта"), то скорее всего такой процессор уже "заряжен"
  - Процессоры без TrustZone уязвимы (небезопасны)
- "Движки" большинства мобильных, встраиваемых ОС (iOS, Android, Tizen, Sailfish построены на ядре Linux
  - При инициализации устройства ядро обращается к механизмам TrustZone (Secure Monitor Call - внешне ничем не примечательная команда SMC #0)
    - Без этого ядро просто не запустится (инициализация кэш L2, управление питанием и пр.)
- Сертифицированные ОС для ARM-процессоров из своего ядра имеют множественные вызовы SMC #0
  - Примеры:
    - Android 6.0 Marshmallow
    - Ядро Astra Linux Special Edition 1.4 (релиз “Новороссийск” для ARM)
    - Ядро Linux 4.5



Эффективна ли сертификация ОС и приложений?

Защищённые смартфоны

- Коперник С1
  - Процессор: Qualcomm Snapdragon MSM 8960
  - ОС: Android 4.2.2
- Samsung Z3
  - Процессор: Qualcomm Snapdragon MSM 8916
  - ОС: Tizen
- YotaPhone, YotaPhone 2
  - Процессор: Qualcomm Snapdragon MSM 8960 / MSM 8974
  - ОС: Android 4.2.2 / Android 4.4, 5.0

Везде есть вызовы SMC #0

Примеры "заряженных" процессоров и аппаратов

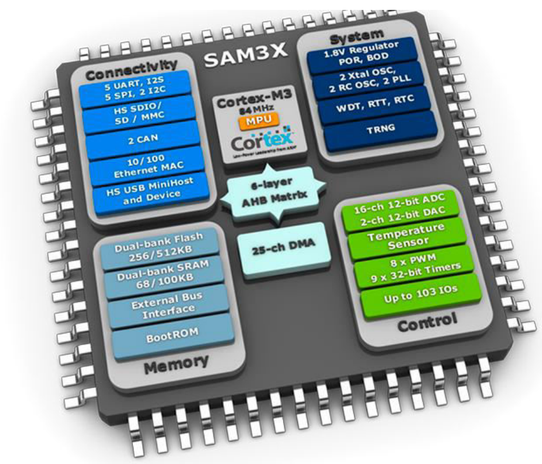
- Процессоры с "заряженной" TrustZone (исследованные нами)
  - Qualcomm MSM8660, MSM8960, MSM8974, APQ8064, APQ8084
  - NVidia Tegra 4
  - Cavium Thunder (для сетевого оборудования и дата-центров)
  - Spreadtrum sc9836 (для смартфонов)
  - Samsung Exynos 7
  - Rockchip rk3368 (для set-top box)
  - Mediatek MT6795, MT8173
  - HiSilicon Kirin 620

Ядро Linux 4.5

- Примеры "заряженных" аппаратов
  - Google Nexus 6, Nexus 7
  - Samsung Galaxy Note, Samsung Galaxy Note 3, Samsung Galaxy S4 Active, Samsung Galaxy S4 I9505, Samsung Galaxy S4 LTE, Samsung Galaxy Note 4, Samsung Galaxy Note Edge, Samsung Galaxy S5, Samsung Galaxy S5 Plus
  - LG Connect 4G, LG Optimus LTE LU6200, LG Lucid, LG Spectrum II 4G (VS930), LG Escape (P870), LG Optimus LTE II, LG G2, LG Optimus G Pro, LG G Pad, LG G Pad 8.3, LG G3
  - Sony Xperia GX, Sony Xperia SX, Sony Xperia V, Sony Xperia Z1
  - HTC Evo 3D, HTC Evo 4G LTE, HTC Droid Incredible 4G LTE, HTC One XL, HTC One, HTC Butterfly S, HTC One Max
  - Xiaomi MI-One, Xiaomi Mi-2S
  - Asus Transformer Pad Infinity, Asus Padfone Infinity
  - ZTE V96, ZTE Grand Memo, ZTE Nubia Z5S mini
  - Motorola Droid RAZR M, Motorola Droid RAZR HD, Motorola RAZR MAXX HD
  - Pantech Vega Racer, Pantech Sky LTE EX, Pantech Burst
  - Huawei Ascend P1 LTE,…

Что сделано

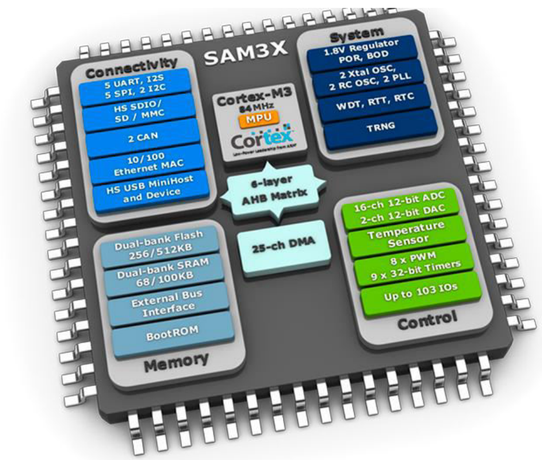
- Глубоко изучена проблематика TrustZone
  - Исследовано большое количество ARM-процессоров, ядер мобильных и встраиваемых ОС, механизмов вызовов и работы TrustZone (TEE)
  - Найдены процессоры с открытой TrustZone и вендоры, готовые предоставить всю необходимую документацию, "открыть" загрузчики и поставлять такие чипы



- Разработана собственная реализация микроядерной ОС для TrustZone и набор механизмов для общения с RichOS
  - Делаем модуль доверенной загрузки (первая команда после включения питания наша) - Aladdin TSM (для ARM)
  - Портируем виртуальный токен в TrustZone, прикладным приложениям предоставим обычный pkcs#11 интерфейс как для обычного токена (JaCarta-2 ГОСТ)

Что это даёт

- Доверенная аппаратно-программная Платформа
  - Возможность использования самой современной зарубежной элементной базы
    - В т.ч. в качестве альтернативы российской (перспективы развития пока непонятны, т.к. заводы попали под санкции)
  - Возможность повышения уровня доверия при сертификации (в т.ч. на ГТ)
  - Возможность полного контроля всего процесса обмена, хранения и обработки информации
- Технология "стерилизации"
  - Возможность использования существующих устройств без изменения их схемотехники
  - Совместимость и преемственность со всем уже разработанным ПО - гостевые ОС и приложения
- Возможности применения
  - Доверенное терминальное оборудование, планшеты, смартфоны, M2M, IoT, АУС ТП, встраиваемая электроника, навигация, платёжные терминалы, медицинские приборы, роутеры, коммуникационное оборудование и пр.



Аладдин

Будь собой в электронном мире!

Будь собой в электронном мире!

Лицензии ФСТЭК России № 0037, № 0054, № 2874
Лицензии ФСБ России № 12632Н, № 24530
Сертификат соответствия системы управления качеством СМК ГОСТ Р ИСО 9001-2011
№ РОСС RU.ИС72.К00082 от 10.07.15

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru

Приведённая информация актуальна по состоянию на 7 февраля 2017 г.