Securing IoT Devices using Arm TrustZone®

Class 2: Introduction to Arm TrustZone

November 27, 2018

Jacob Beningo

DesignNews

CEC CONTINUING EDUCATION CENTER

Presented by: Digi-Key ELECTRONICS

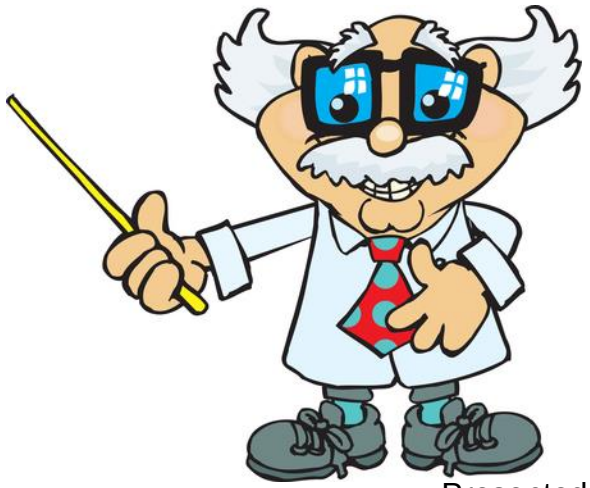
Course Overview

Topics:

- Understanding Embedded System Security
- **Introduction to Arm TrustZone®**
- Creating your First TrustZone Application
- Designing and Debugging a Secure Boot Solution
- Securing a RTOS Application with TrustZone

Session Overview

- Arm TrustZone Security Extension
- Cortex-M23/M33 Overview
- Programmers Model



Presented by:

Arm TrustZone Technology

Security extension for the Armv8-M architecture

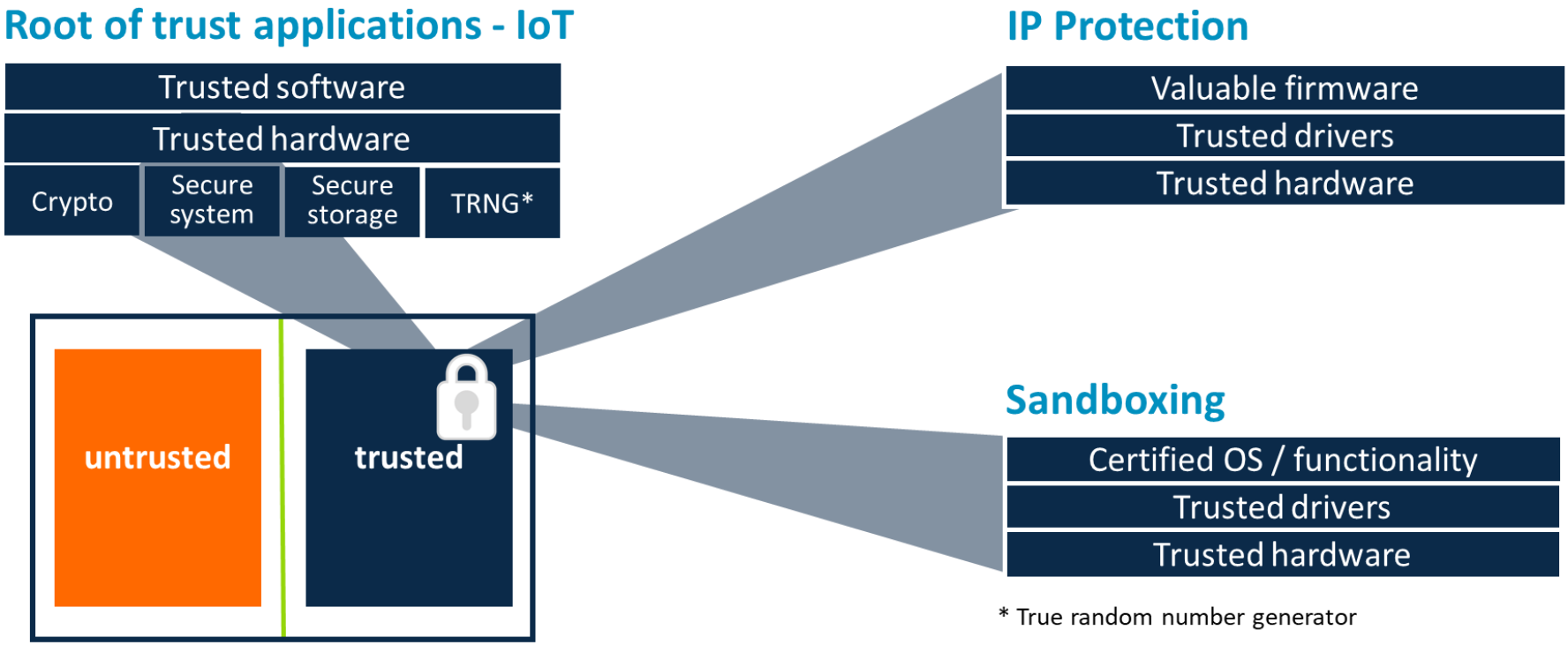
- Security architecture for deeply embedded processors
- Enables containerisation of software
- Simplifies security assessment of embedded devices.

Conceptually similar and compatible with existing TrustZone technology

- New architecture tailored for embedded devices
- Preserves low interrupt latencies of Cortex-M processors
- Provides high performance cross-domain calling.

arm TRUSTZONE

Efficient Security for embedded applications

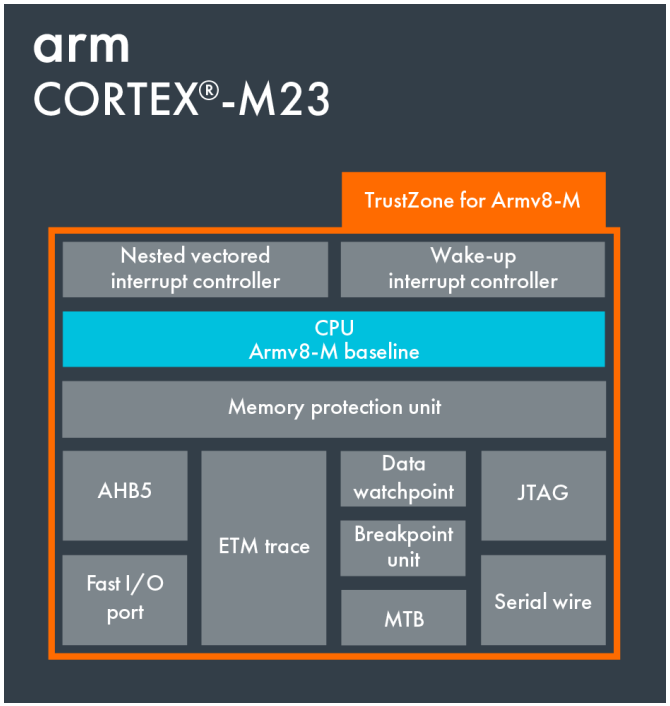


Cortex-M23: Ultra low-power with TrustZone

Smallest area, lowest power
- With TrustZone, same energy efficiency as Cortex-M0+

Ultra-high efficiency
- Flexible sleep modes
- Extensive clock gating
- Optional state retention

Enhanced capability
- Increased performance
- Multi-core system support
- 240 interrupts
- Hardware stack checking



Security foundation
- System wide security with TrustZone technology

Enhanced memory protection
- Easy to program
- Dedicated protection for both secure and non-secure states

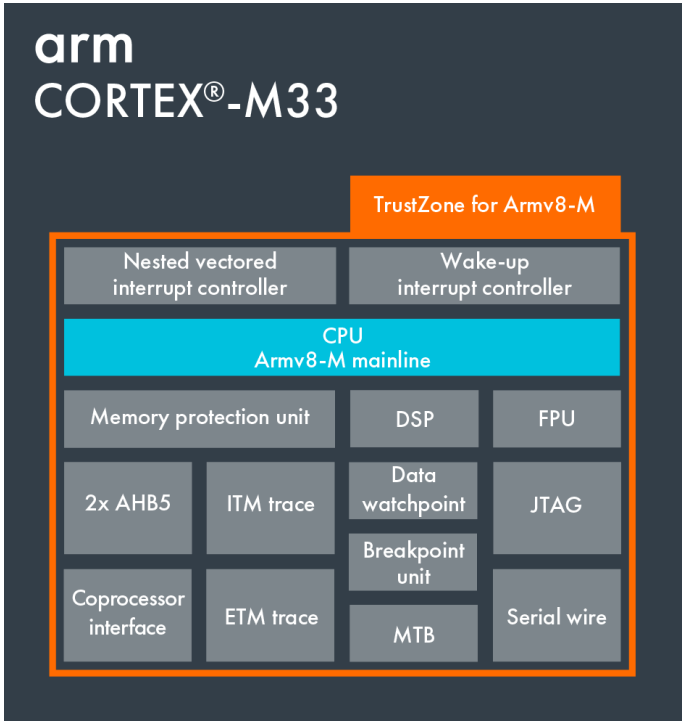
Enhanced & secure debug
- Security aware debug
- Simplified firmware development
- Embedded trace macrocell

Cortex-M33: High Performance with TrustZone

32-bit processor of choice
- Optimal balance between performance and power
- 20% greater performance than Cortex-M4
- With TrustZone, same energy efficiency as Cortex-M4

Digital signal control
- Bring DSP to all developers
- FPU offering up to 10x performance over software

Extensible compute
- Co-processor interface for tightly-coupled acceleration



Security foundation
- System-wide security with TrustZone technology

Enhanced memory protection
- Easy to program
- Dedicated protection for both secure and non-secure states

Enhanced & secure debug
- Security aware debug
- Simplified firmware development

TrustZone Overview

arm TRUSTZONE

Normal environment (Non-Secure)

Application Examples

- User applications
- RTOS
- Device drivers
- Protocol stacks

Normal Resources

- General peripherals

Handler Mode

Thread Mode

Handler Mode

Thread Mode

Protected environment (Secure)

Secure Software Examples

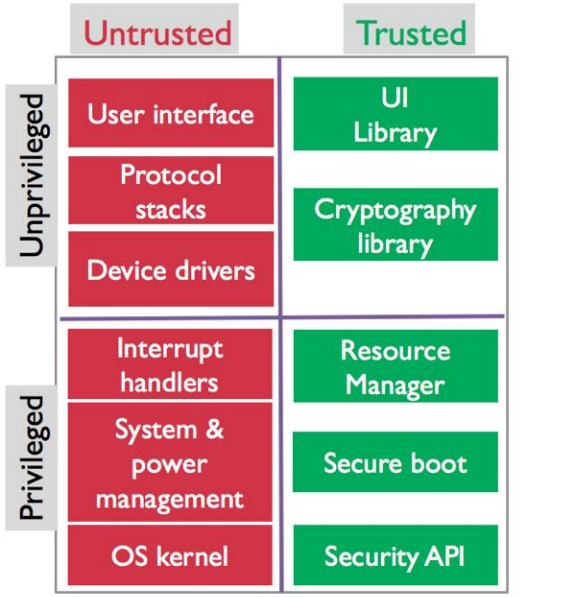
- Secure Boot
- Cryptography libraries
- Authentication
- RTOS support APIs / RTOS

Secure Resources

- Secure storage
- Crypto accelerators

Software Component Organization

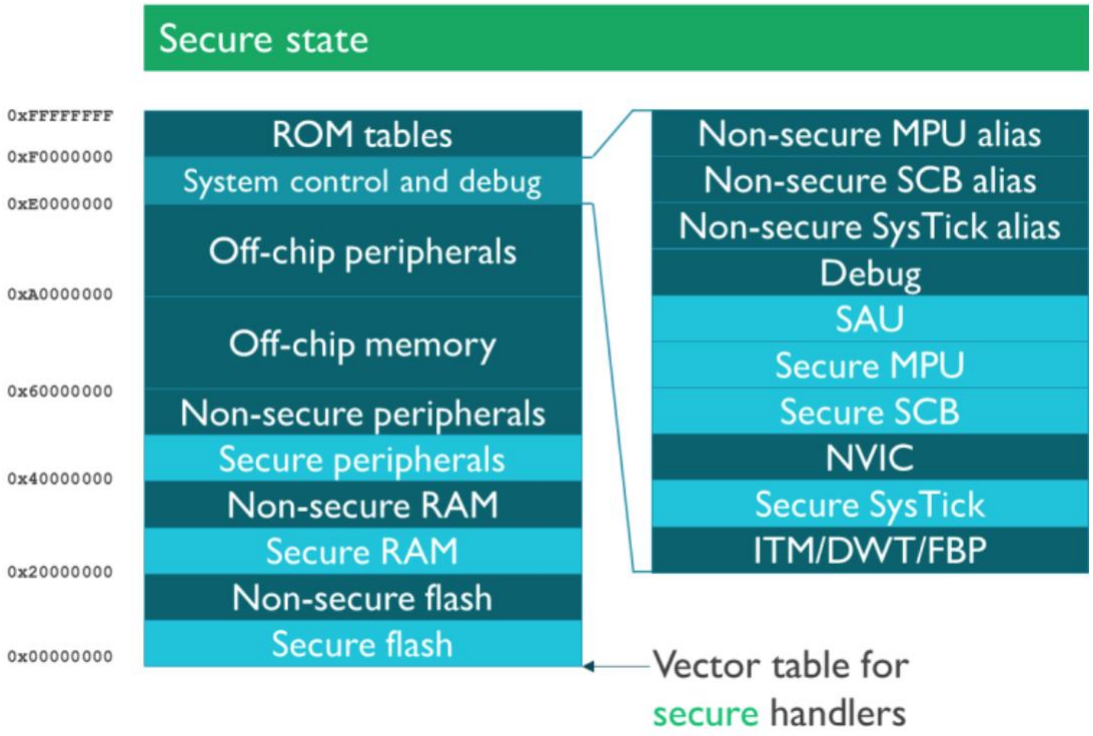
Traditional Developer Design



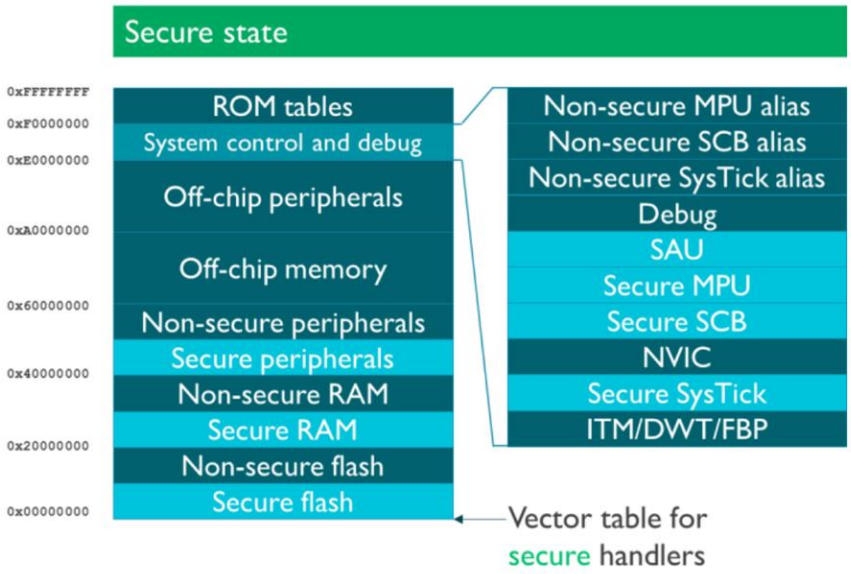
New additional security

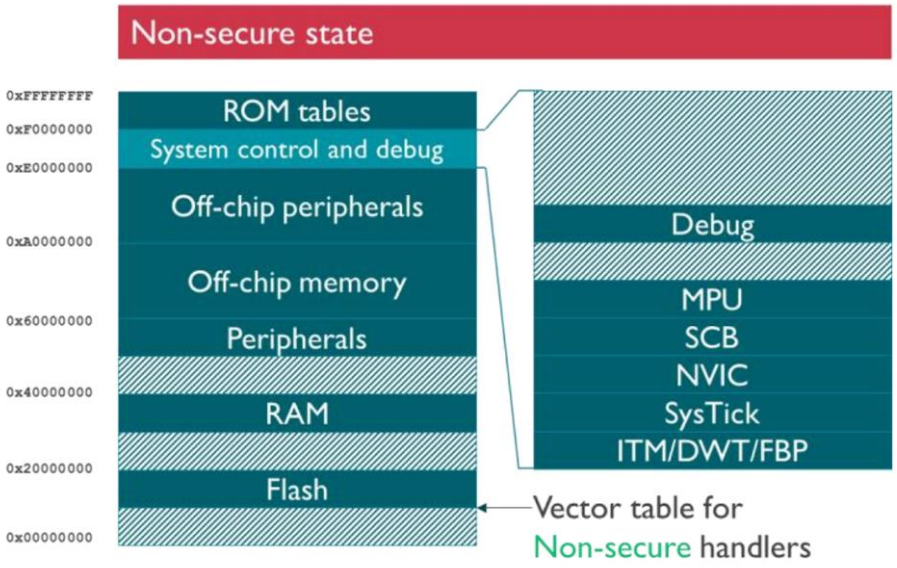
Secure State Programmers Model

- All peripherals and memory can be accessed
  - Secure and Unsecure
- Security Attribution Unit (SAU)
  - Configures non-secure peripherals, memory, etc

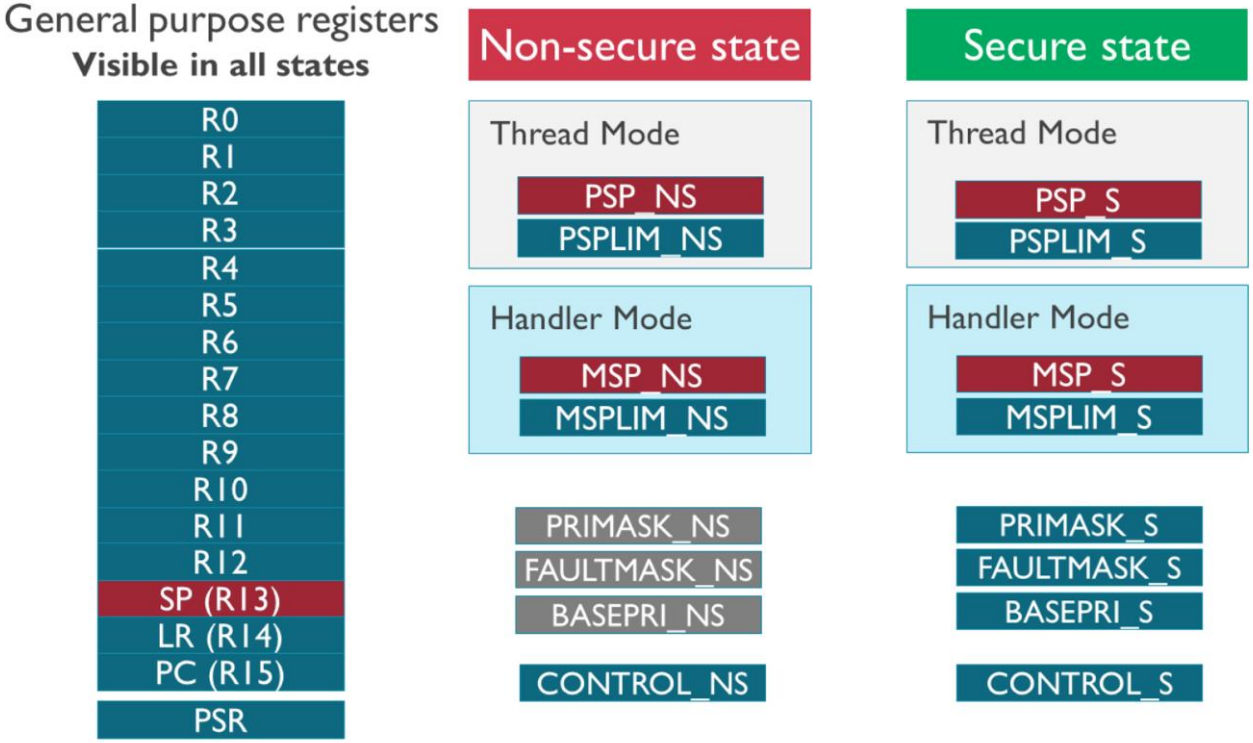


Secure and Non-secure Comparison

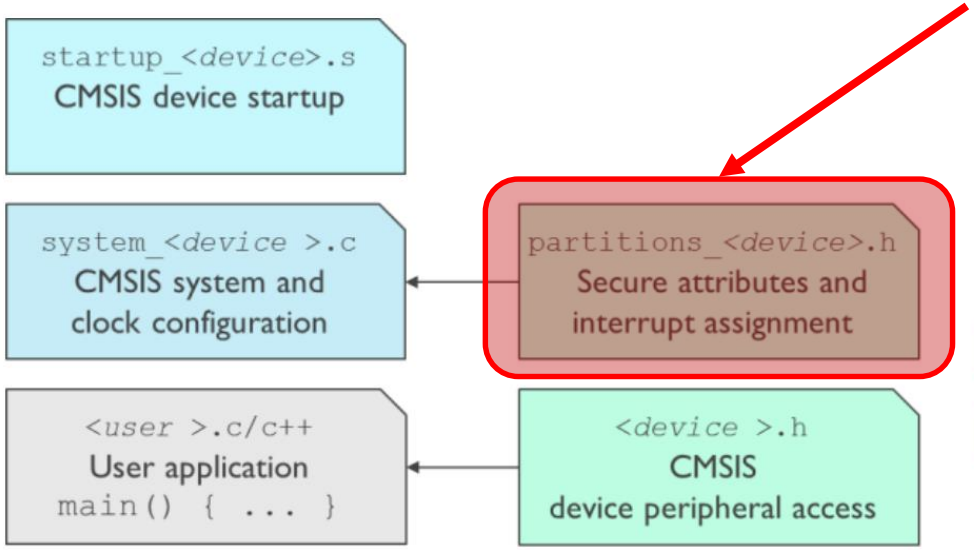




Core Registers



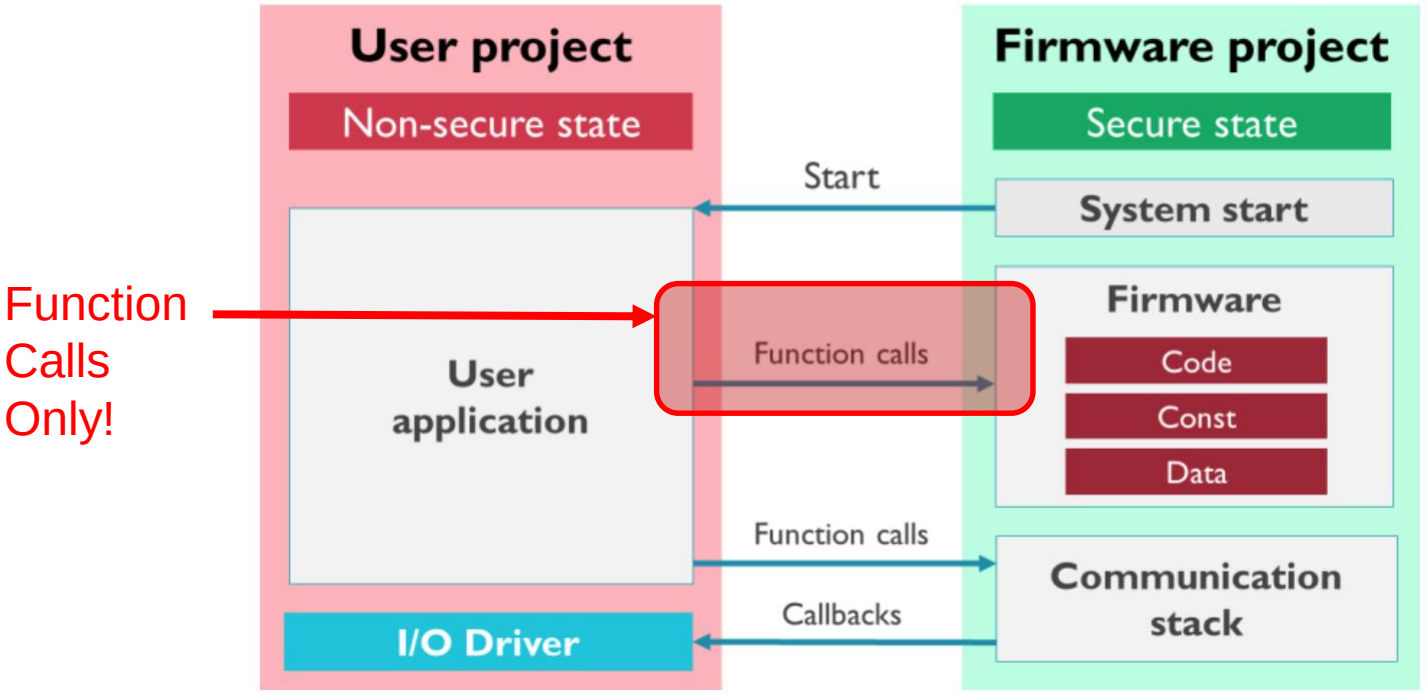
CMSIS Partitions



Initial setup of the non-secure memory map

- Provide settings for the SAU CTRL register.
- Configure the SAU Address Regions.
- Configure device-specific deep sleep and exception settings.
- Configure device-specific interrupt target settings.

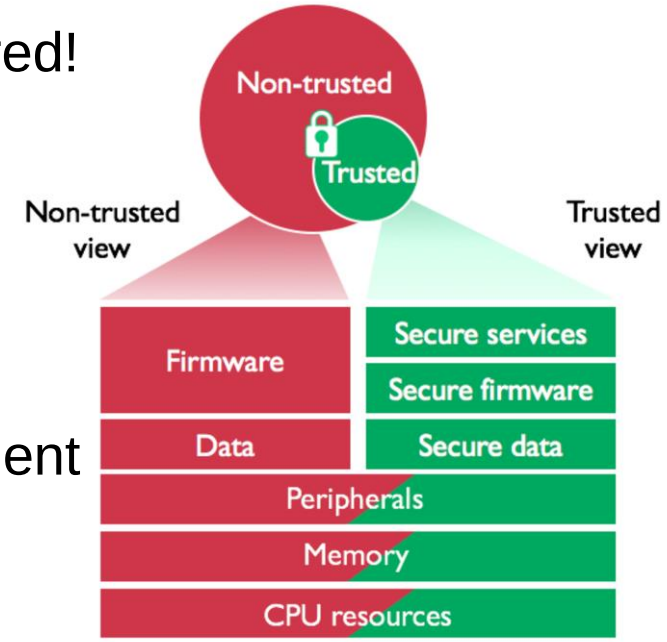
General Application Example



TrustZone – Real-Time Transition

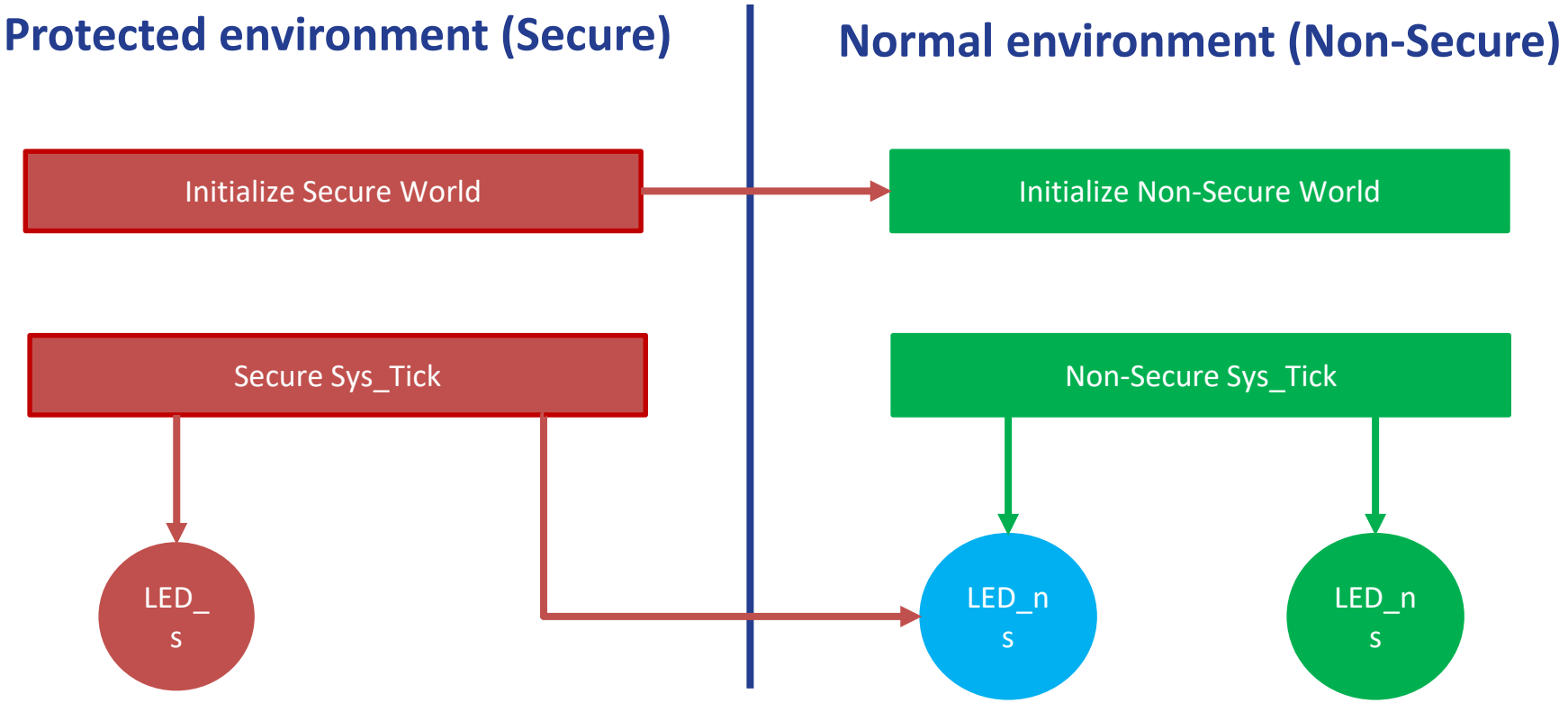
Hardware Isolation – No Software Required!

- CPU instruction automatically inserted
- Worst case overhead 2 clock cycles
- Deterministic response
- Extra overhead is application independent
  - Parameter, pointer testing
  - etc



*≤2 cycles

General Application Example - LED



Additional Resources

- Download Course Material for
  - C/C++ Doxygen Templates
  - Example source code
  - Blog
  - YouTube Videos
- Embedded Bytes Newsletter
  - http://bit.ly/1BAHYXm

From www.beningo.com under

- Blog > CEC – Securing IoT Devices using Arm TrustZone