Securing IoT Devices using Arm TrustZone®

Class 5: Securing a RTOS Application with TrustZone

November 30, 2018

Jacob Beningo

DesignNews

CEC CONTINUING EDUCATION CENTER

Presented by: Digi-Key ELECTRONICS

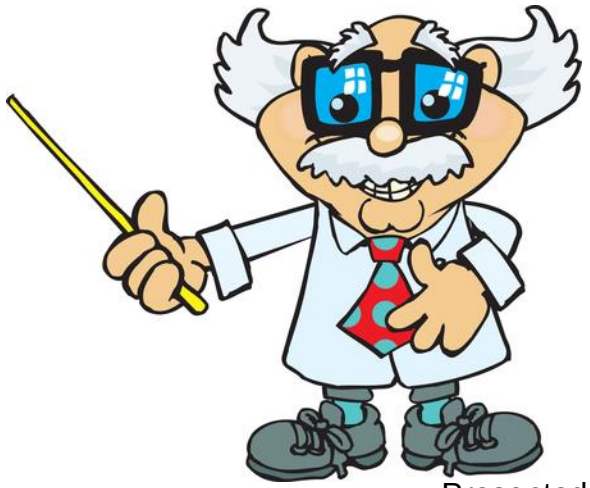
Course Overview

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

- Enter the RTOS
- RTOS options
- RTOS thread management
- RTOS example application
- Course review



Presented by:

General Application Example

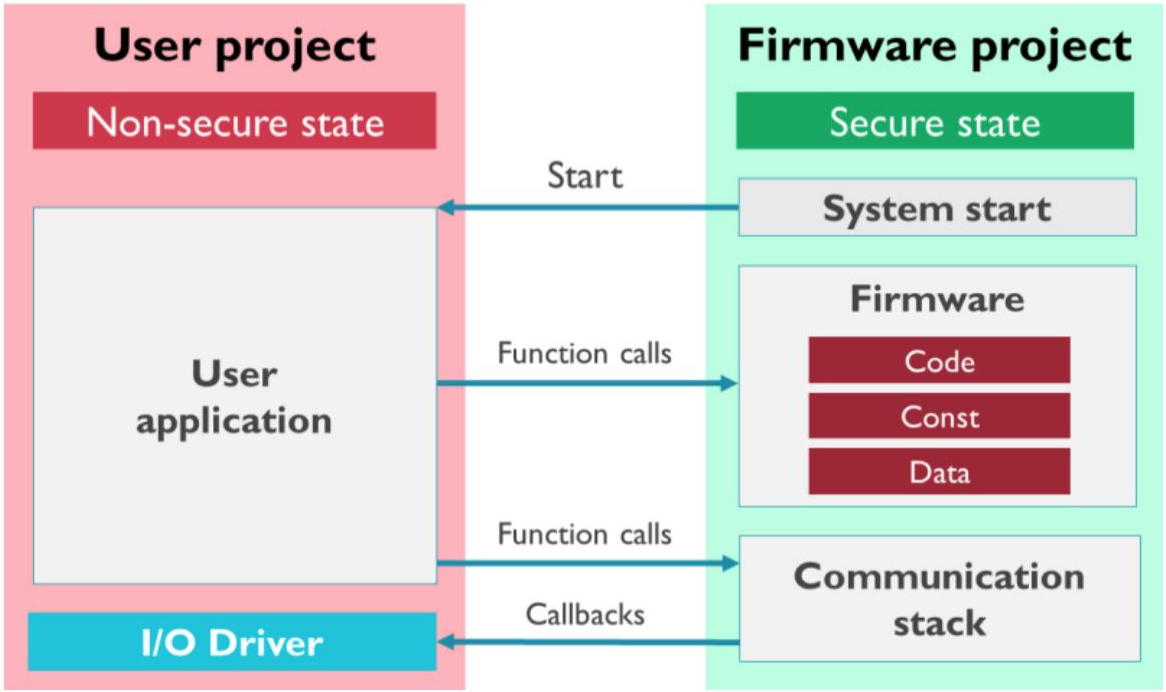


Image Source: Keil AN291

Real-time Operating Systems

- Provide applications with the ability to execute multiple threads or tasks in parallel
- Priority based
- Many allow memory management capabilities

Should the RTOS go in secure or non-secure code?

RTOS Option #1

Non-secure state	Secure state
• User Application • Tasks • RTOS Kernel • RTOS Objects • etc	• Secure Library Functions • Communication Stacks • etc

RTOS Option #2

Non-secure state	Secure state
• User Application • Tasks • RTOS Kernel • RTOS Objects • etc	• Secure Application • Tasks • RTOS Kernel • RTOS Objects • etc

RTOS Option #3

Non-secure state	Secure state
• User Application • Tasks • RTOS Kernel • RTOS Objects • etc	• Secure Library Functions • Communication Stacks • System Monitor • Time Scheduler

RTOS Thread Management

Non-secure state

RTOS_NS

- RTOS API functions
- Thread scheduler with SysTick handler
- Resource handling for non-secure objects

Secure state

RTOS_S (secure part)

- Context switch to handle secure state registers
- Called by RTOS_NS
- Manages thread stack (PSP_S)

RTOS Thread Management

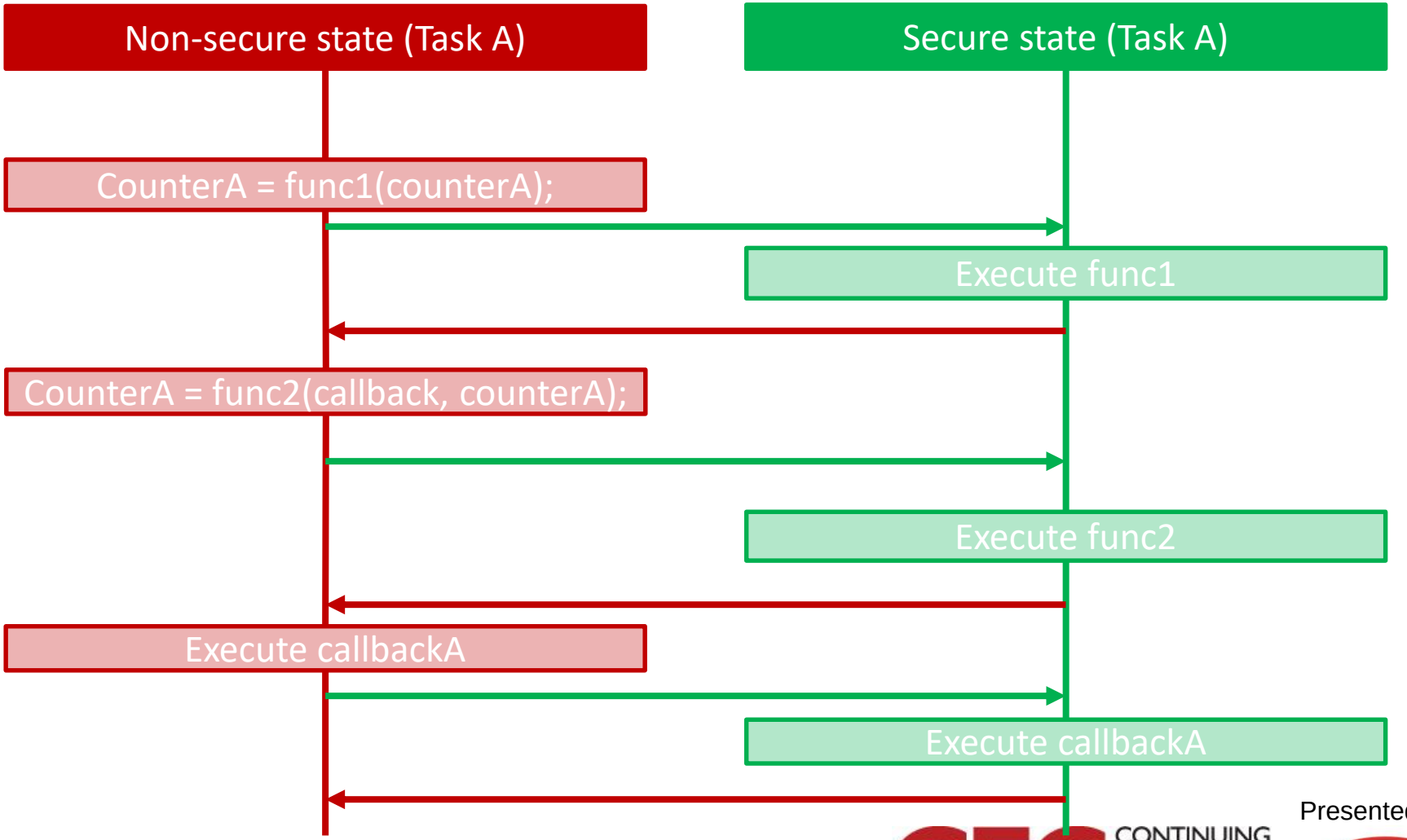
In the non-secure state:

- Tasks are started
- Tasks are executed
- All API's are available

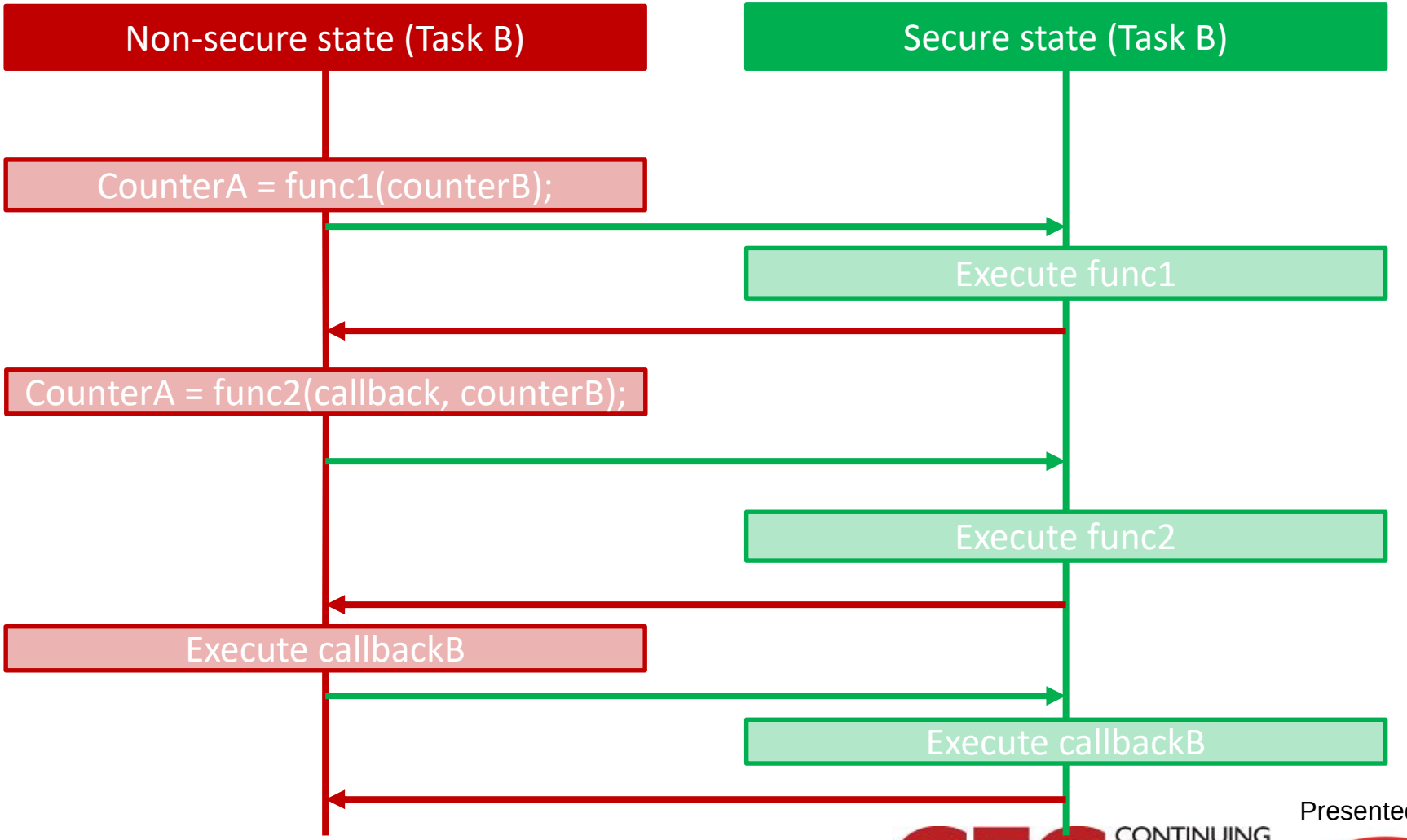
In the secure state:

- Task stacks are allocated
- Access to secure memory

RTOS Example Application



RTOS Example Application



Security is not optional anymore

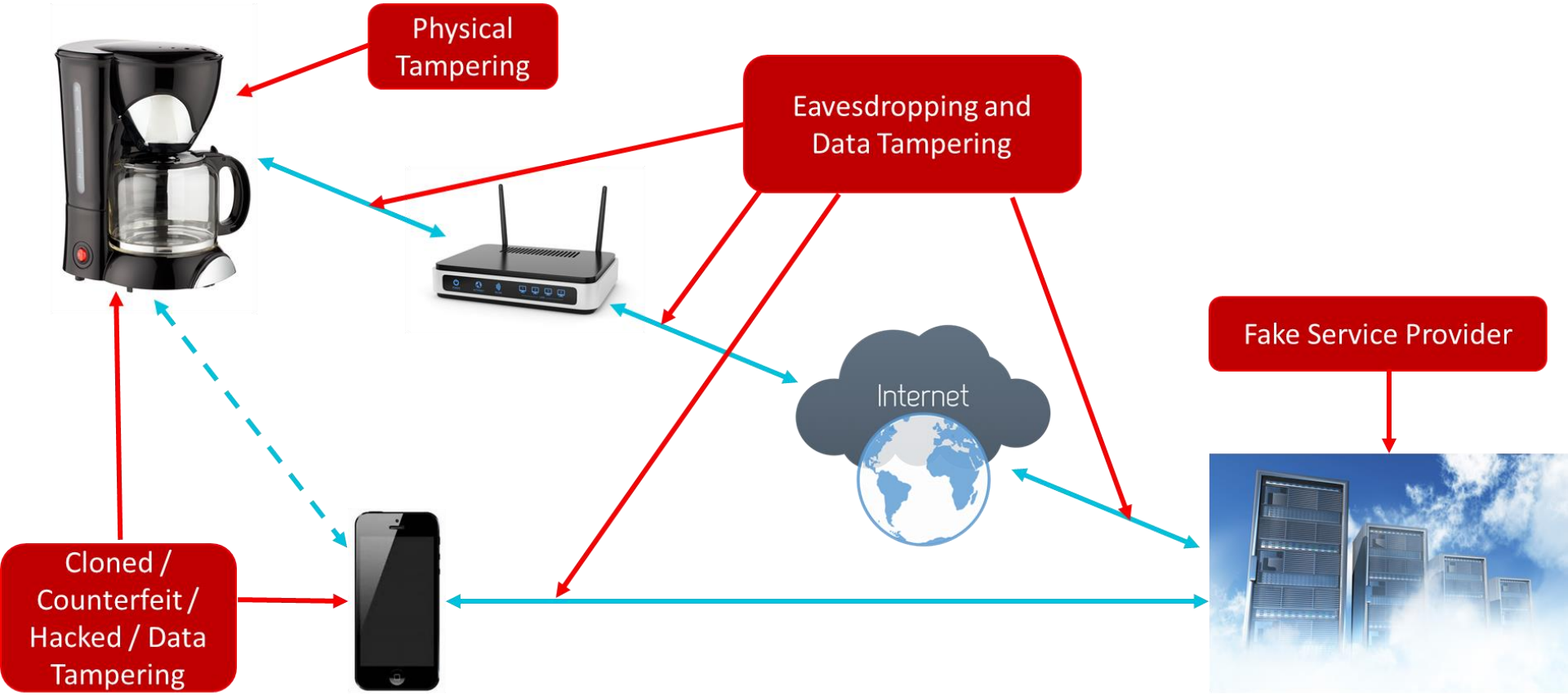
Billions of IoT devices

Data integrity, security & privacy

Potential losses of hacks, breaches

Image Source: Arm

There are multiple ways to attack



arm TRUSTZONE

Normal environment (Non-Secure)

Application Examples

- User applications
- RTOS
- Device drivers
- Protocol stacks

Normal Resources

- General peripherals

Handler Mode

Thread Mode

Protected environment (Secure)

Handler Mode

Thread Mode

Secure Software Examples

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

Secure Resources

- Secure storage
- Crypto accelerators

Where to go from here?

- Get hands-on with TrustZone
- Get several development boards and explore the different implementations
- Read the Keil AN291
- Visit Beningo.com and read my TrustZone blogs
- Join me for my TrustZone Technology primer

Where to go from here?

Microchip SAM L11 Xplained Board

arm KEIL

Atmel Studio 7

A light snack …

Presented by:

CEC CONTINUING EDUCATION CENTER

Digi-Key ELECTRONICS

DesignNews

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