Securing IoT Devices using Arm TrustZone®

Class 1: Understanding Embedded System Security

November 26, 2018
Jacob Beningo

DesignNews

Presented by:

CEC CONTINUING EDUCATION CENTER

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

The Lecturer – Jacob Beningo

Jacob Beningo

Principal Consultant

BENINGO
EMBEDDED GROUP

Social Media / Contact

E	: jacob@beningo.com
T	: 810-844-1522
🐦	: Jacob_Beningo
f	: Beningo Engineering
in	: JacobBeningo
EDN	: Embedded Basics

ARM Connected Community

Consulting

- Advising
- Coaching
- Content
- Consulting
- Training

www.beningo.com

Presented by:

CEC CONTINUING EDUCATION CENTER

Digi-Key ELECTRONICS

Jacobs CEC Courses

CEC 2013 – 2015

- Fundamentals of Embedded Software (2013)
- Mastering the Software Design Cycle (2014)
- Python for Embedded Systems(2014)
- Software Architecture Design (2014)
- Baremetal C (2015)
- Mastering the ARM Cortex-M Processor (2015)
- Writing Portable and Robust Firmware in C (2015)
- Design Patterns and the Internet (2015)

CEC 2016 - 2017

- Bootloader Design for MCUs (2016)
- Rapid Prototyping w/ Micro Python (2016)
- Debugging (2016)
- Professional Firmware (2016)
- API's and HAL's February 2017
- Baremetal to RTOS April 2017
- Designing IoT Sensor Nodes July 2017
- From C to C++ October 2017

CEC 2018

- Connecting Edge Devices (March 2018)
- Building an IoT Connected PLC (April 2018)
- Securing IoT Devices using Arm TrustZone (Nov 2018)
- Minimizing Defects (Dec 2018)

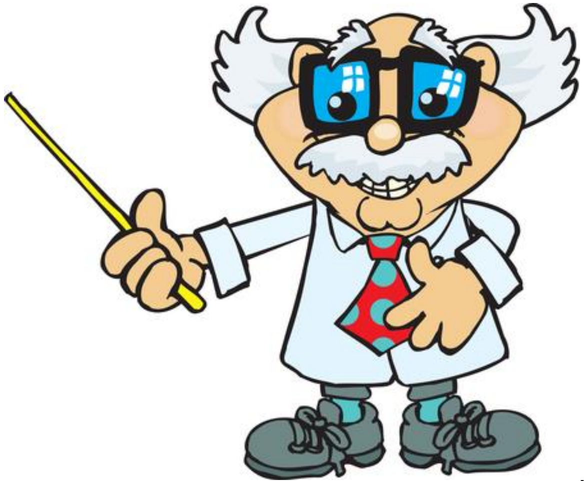
Side Topics 2018

- **TrustZone Technology Primer**
- RTOS Workshop
- Debugging Techniques

Presented by:

Session Overview

- Introduction
- How are systems attacked?
- Attack levels
- Defining a security strategy
- Architectural concepts



Presented by:

World’s Most Dangerous Connected Device?

What is the Worlds Most Dangerous Device?

- The Issues:
  - Safety
  - Security
  - Cost
  - Reliability
  - <u>What else?</u>

Security is not optional anymore

Billions of IoT devices

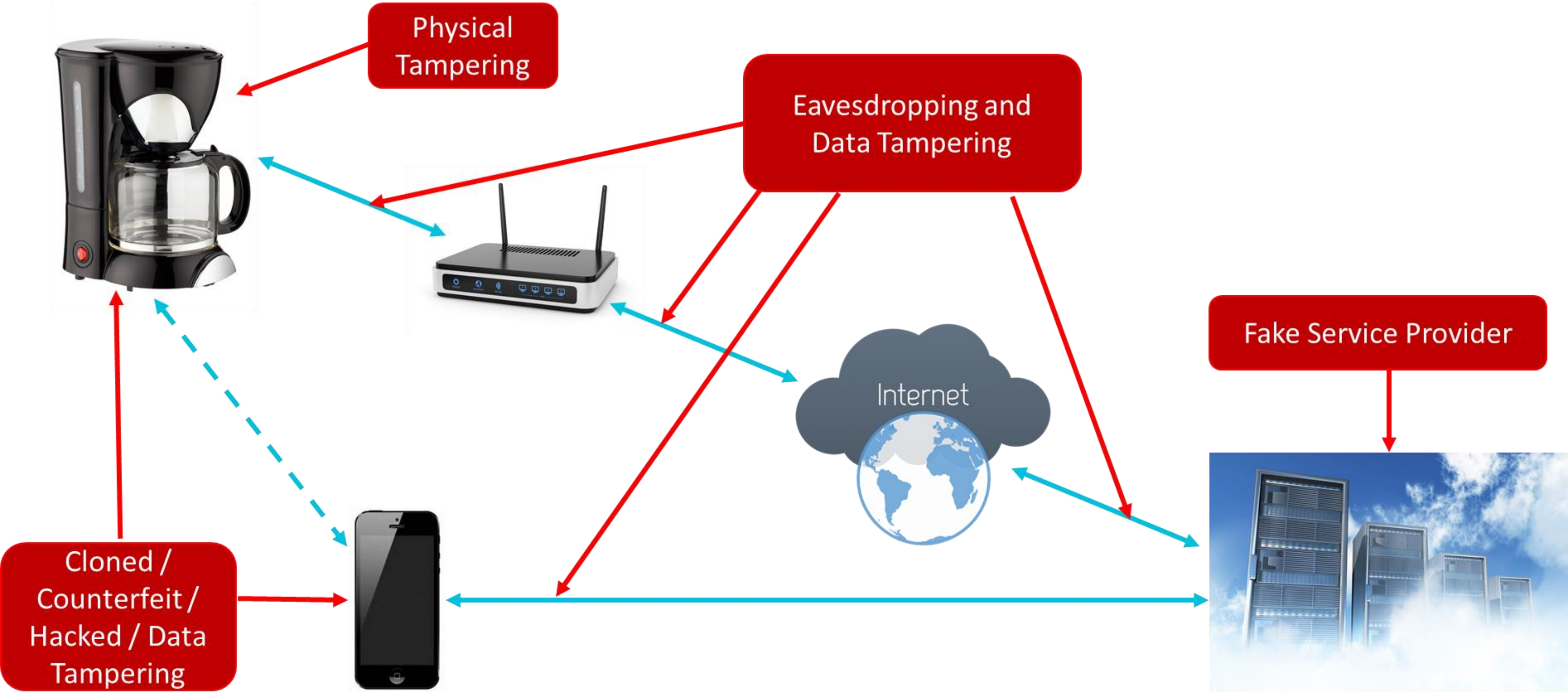
Data integrity, security & privacy

Potential losses of hacks, breaches

Image Source: Arm

Presented by:

Where can attacks come from?



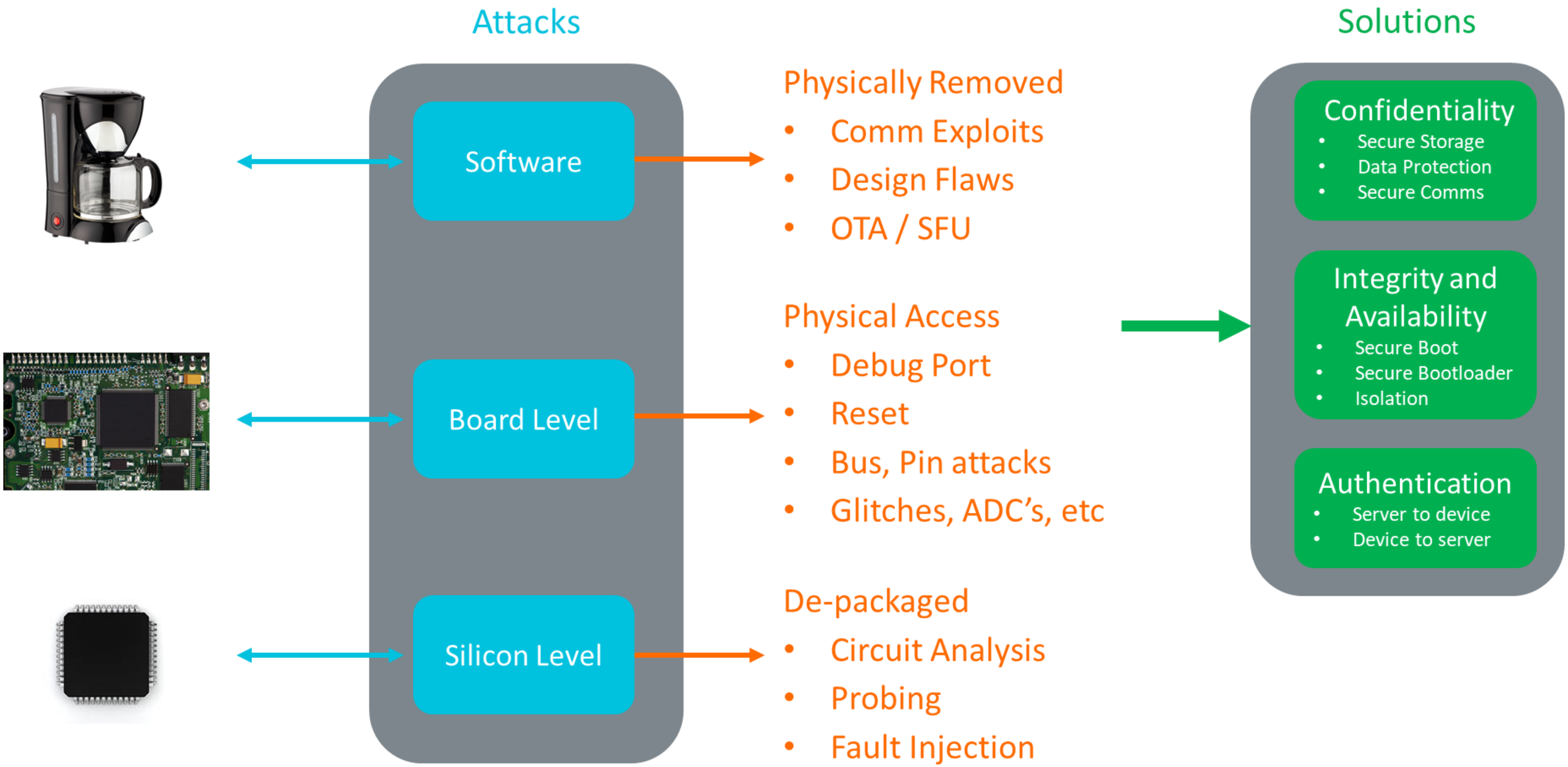
Physical Tampering

Eavesdropping and Data Tampering

Fake Service Provider

Cloned / Counterfeit / Hacked / Data Tampering

Attack Levels



Attacks

- Software
- Board Level
- Silicon Level

Physically Removed

- Comm Exploits
- Design Flaws
- OTA / SFU

Physical Access

- Debug Port
- Reset
- Bus, Pin attacks
- Glitches, ADC's, etc

De-packaged

- Circuit Analysis
- Probing
- Fault Injection

Solutions

Confidentiality

- Secure Storage
- Data Protection
- Secure Comms

Integrity and Availability

- Secure Boot
- Secure Bootloader
- Isolation

Authentication

- Server to device
- Device to server

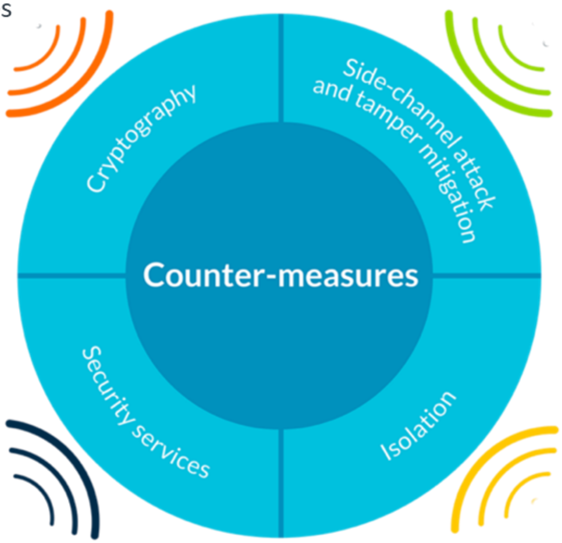
Defining a Security Strategy

Communications

- Man-in-the-middle
- Weak RNG
- Code vulnerabilities

Physical

- Non-invasive – SCA clock/power glitch
- Invasive – probing, laser, FIB



Lifecycle

- Code downgrade
- Change of ownership
- Factory oversupply

Software

- Buffer overflows
- Interrupts
- Malware

Platform Security Architecture

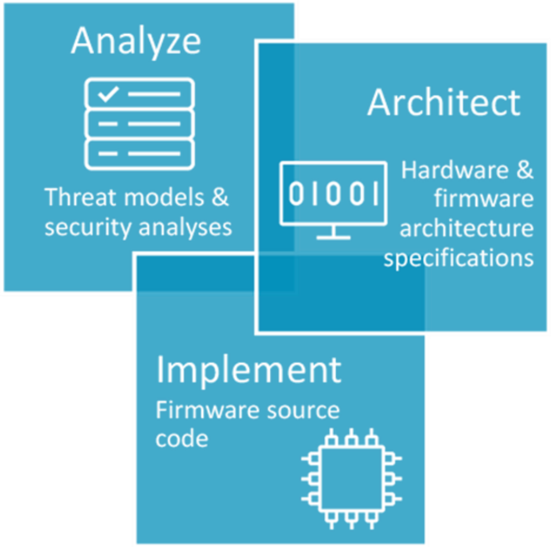
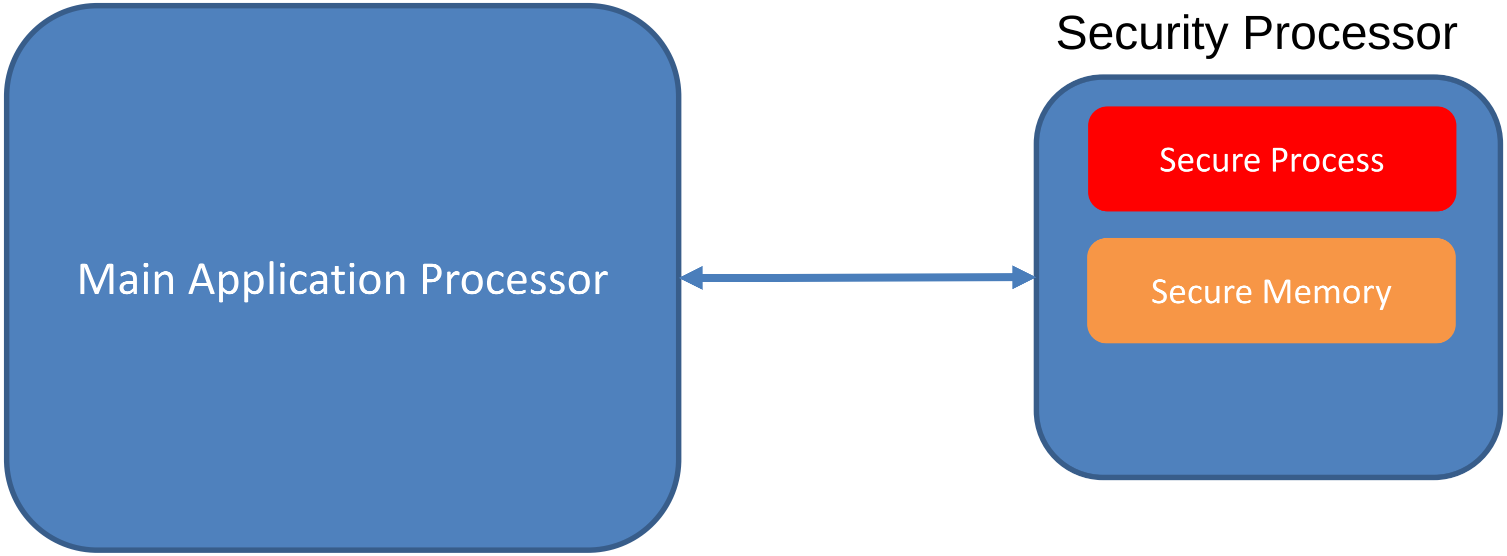
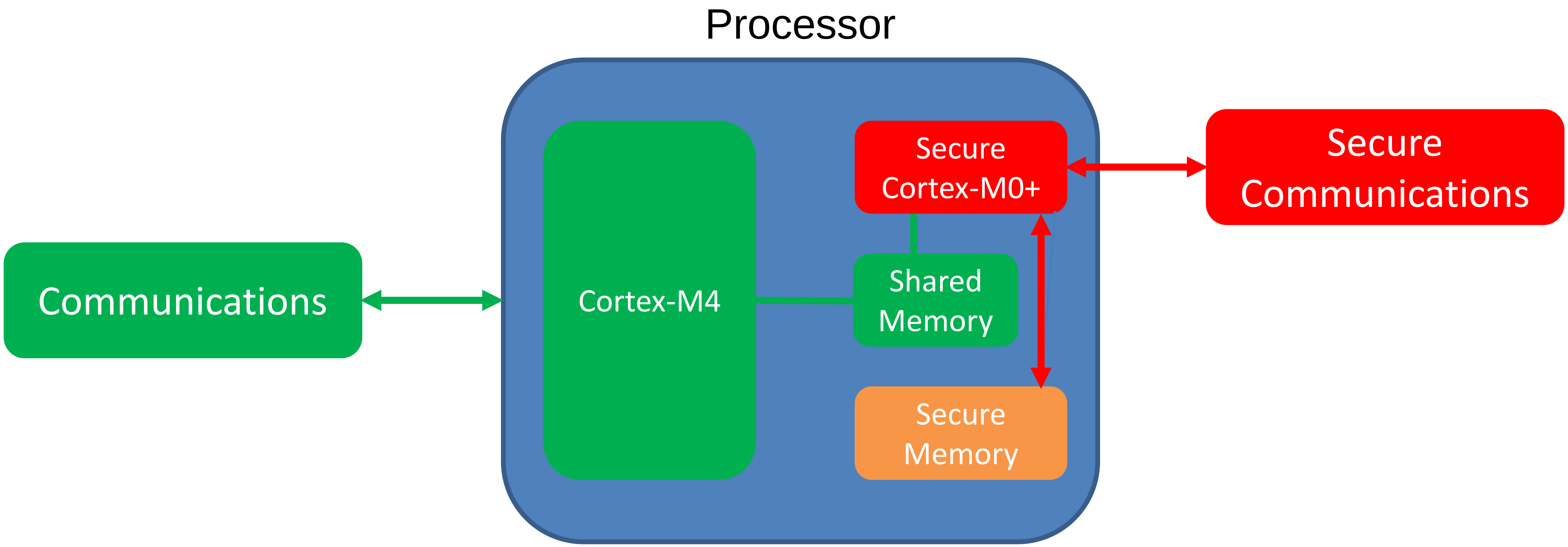

Analyze
Threat models & security analyses
Architect
01001
Hardware & firmware architecture specifications
Implement
Firmware source code

Image Source: Arm

Architecture Concept #1



Architecture Concept #2



Architecture Concept #3

arm TRUSTZONE

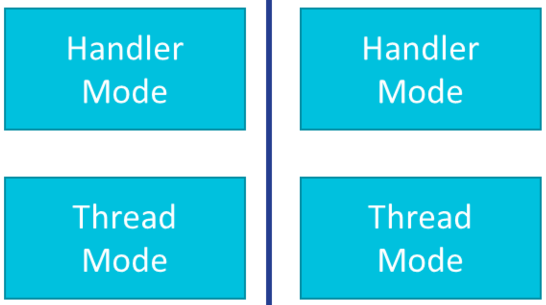
Normal environment (Non-Secure)

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

What You will need …

Microchip SAM L11 Xplained Board

arm KEIL

µVision® 5

Integrated Development Environment

Copyright © 2010-2017 ARM Ltd. All rights reserved.
This product is protected by US and international laws.

ARMKEIL
Microcontroller tools

Atmel Studio 7

A light snack …

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