MCU Security Features for IoT Security

Min-Nan Cheng

Program Director, Microcontroller Application Business Group

nuvoTon

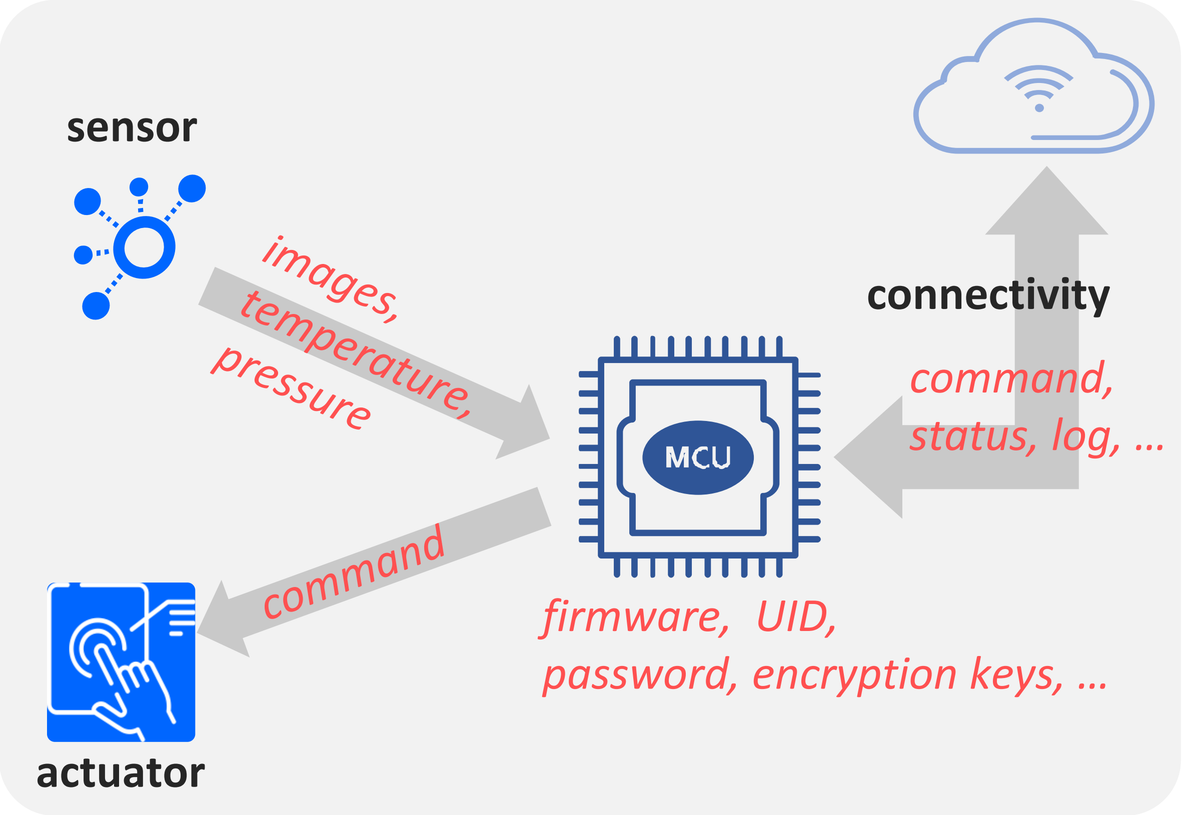
2022 Nuvoton IoT Security Technology Forum | Copyright © 2022 Nuvoton Technology Corporation | Photo by Jeffery Cheng

Content

- Overview to IoT Security
- MCU Security Objectives
- MCU Security Features
- Conclusions

Overview to IoT Security

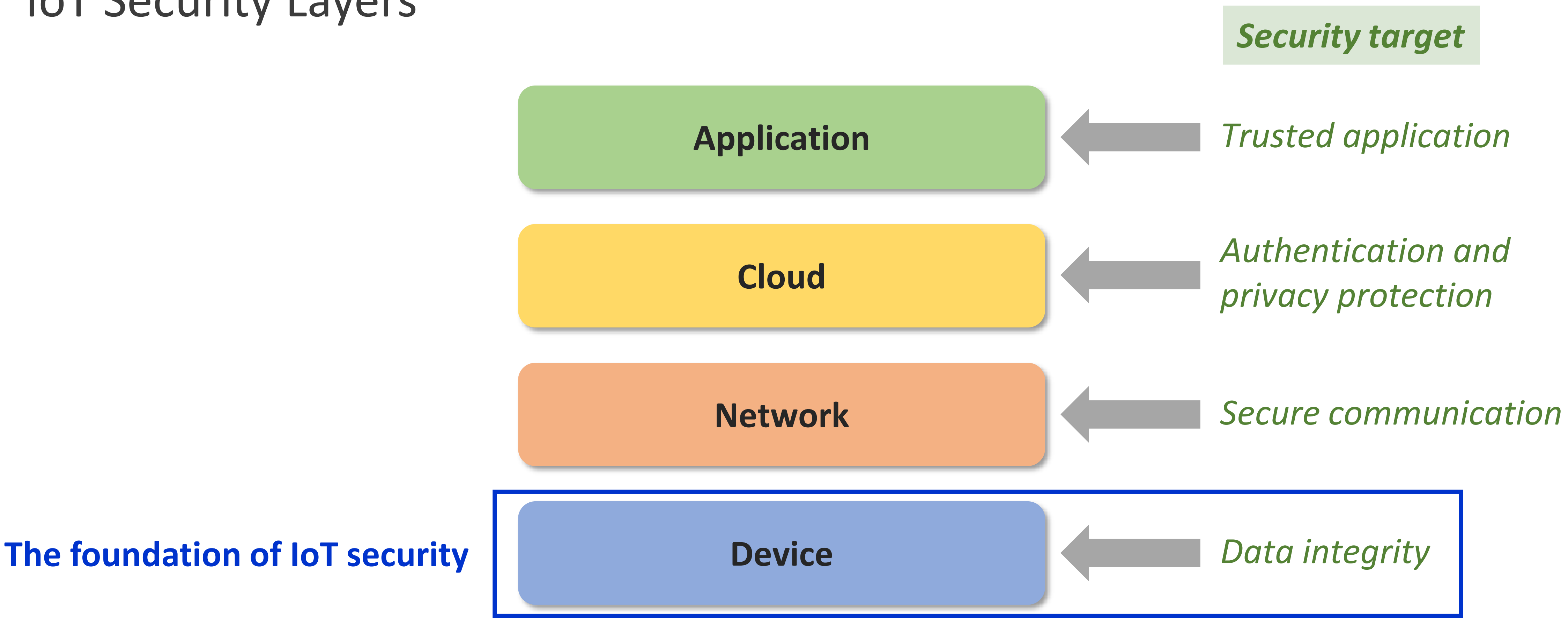
- **IoT Device**
  - Consists of sensor + MCU + actuator
  - Generate and transmit **data**
  - **Data Assets**
    - General
      - Firmware
      - Unique ID
      - Password
      - …
    - Application-specific
      - Sensor data
      - Control data



Data in an IoT Device

Overview to IoT Security

- IoT Security Layers



Security target

Application ← *Trusted application*

Cloud ← *Authentication and privacy protection*

Network ← *Secure communication*

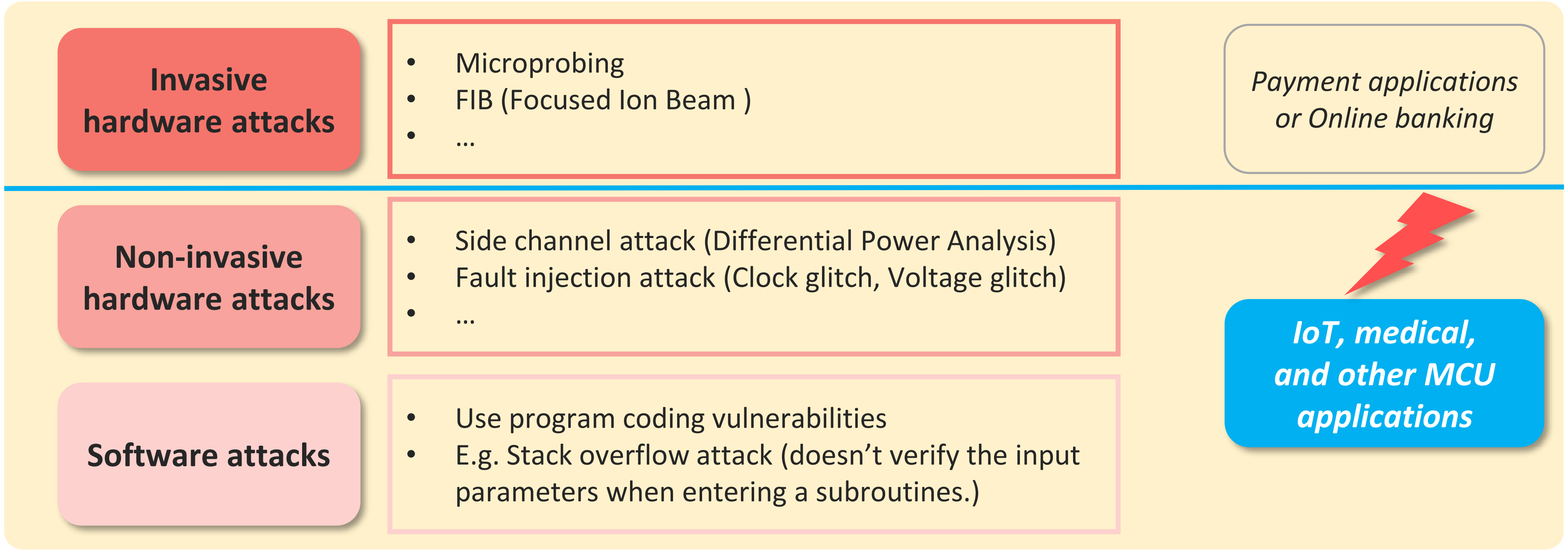
Device ← *Data integrity*

The foundation of IoT security

IoT System Architecture

MCU Security Objectives

- **The Role of MCU in Device Security**
  - Implement the Security Features to defend against **software attacks** and **non-invasive hardware attacks**



Invasive hardware attacks

- Microprobing
- FIB (Focused Ion Beam)
- …

Non-invasive hardware attacks

- Side channel attack (Differential Power Analysis)
- Fault injection attack (Clock glitch, Voltage glitch)
- …

Software attacks

- Use program coding vulnerabilities
- E.g. Stack overflow attack (doesn’t verify the input parameters when entering a subroutines.)

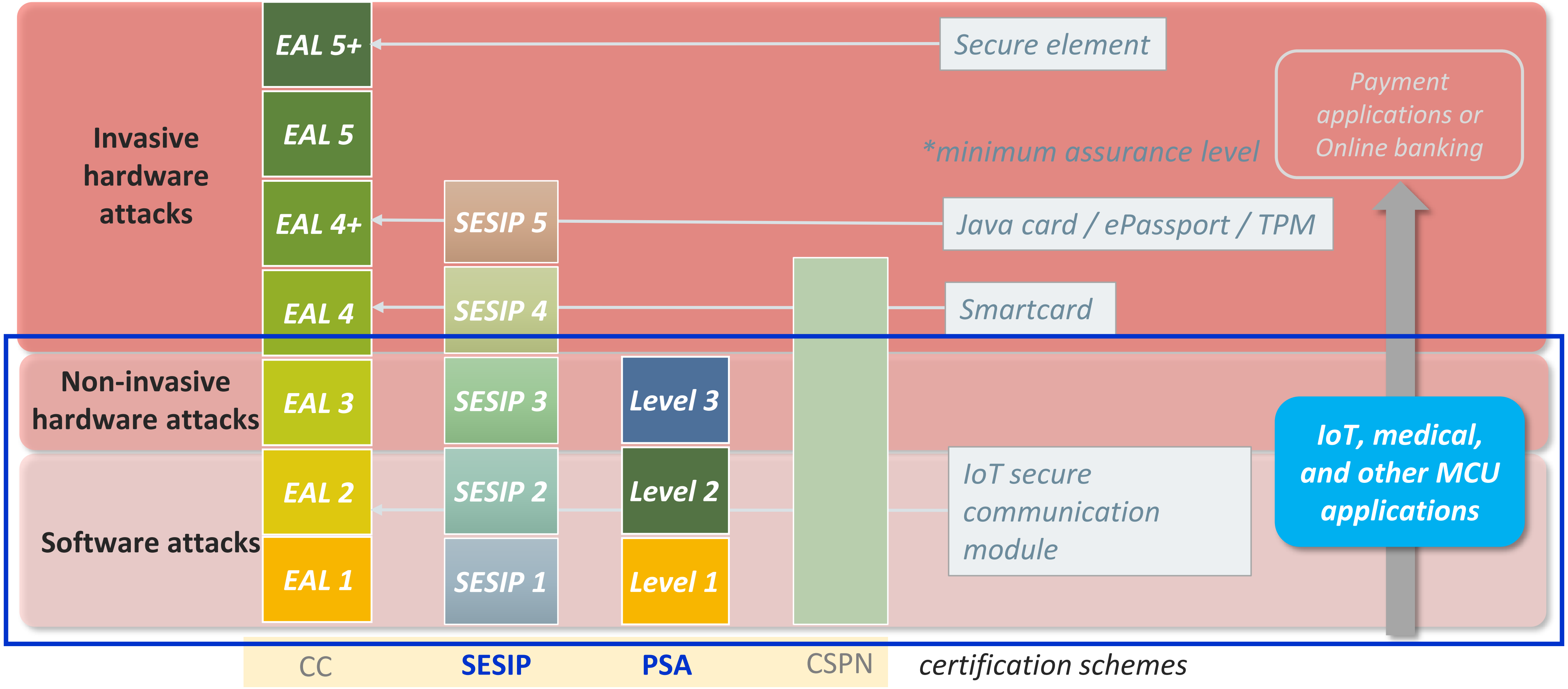
Payment applications or Online banking

IoT, medical, and other MCU applications

Attacks Types on MCU

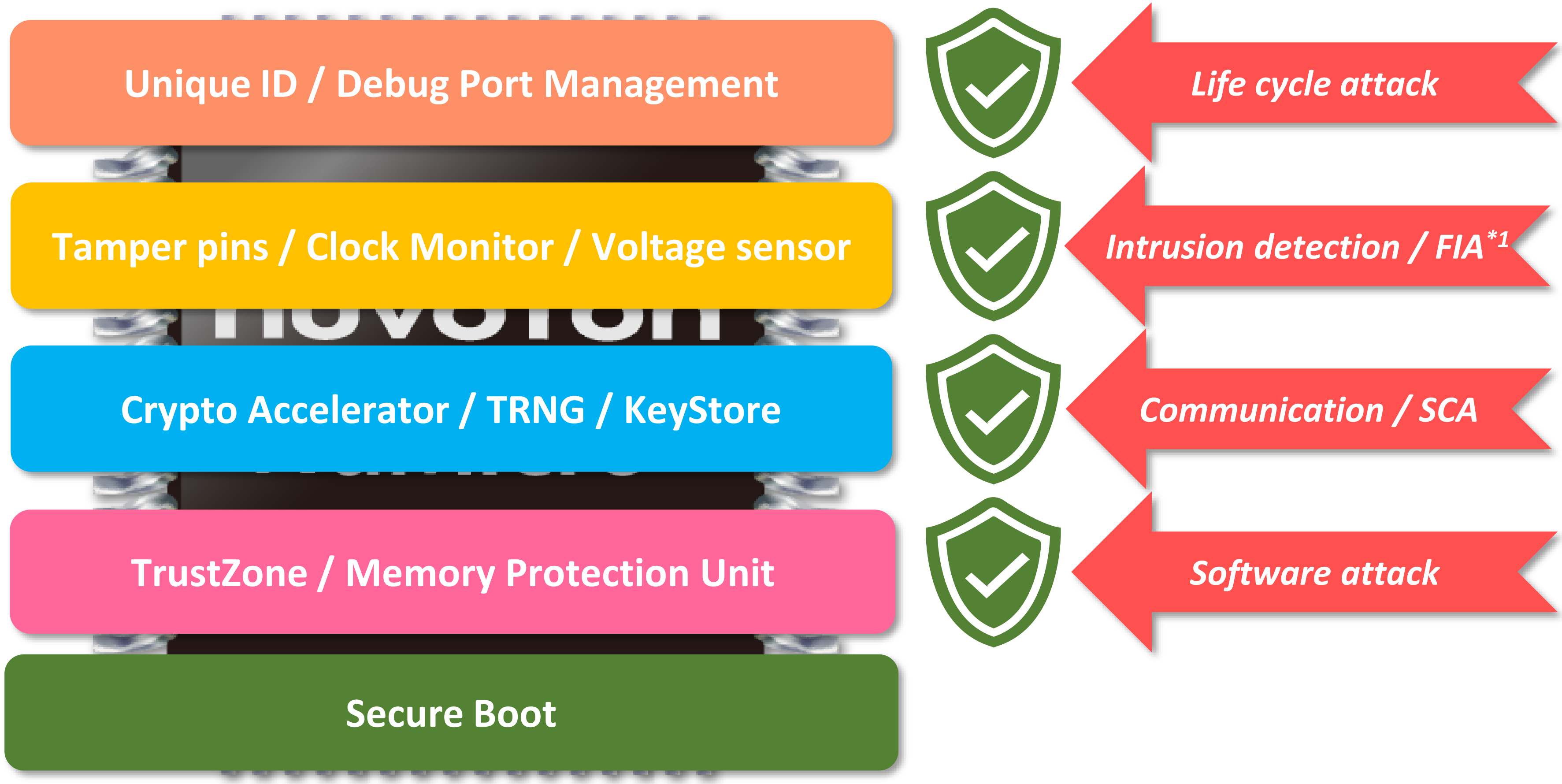
MCU Security Objectives

- Briefing of Security Assurance Levels



MCU Security Features

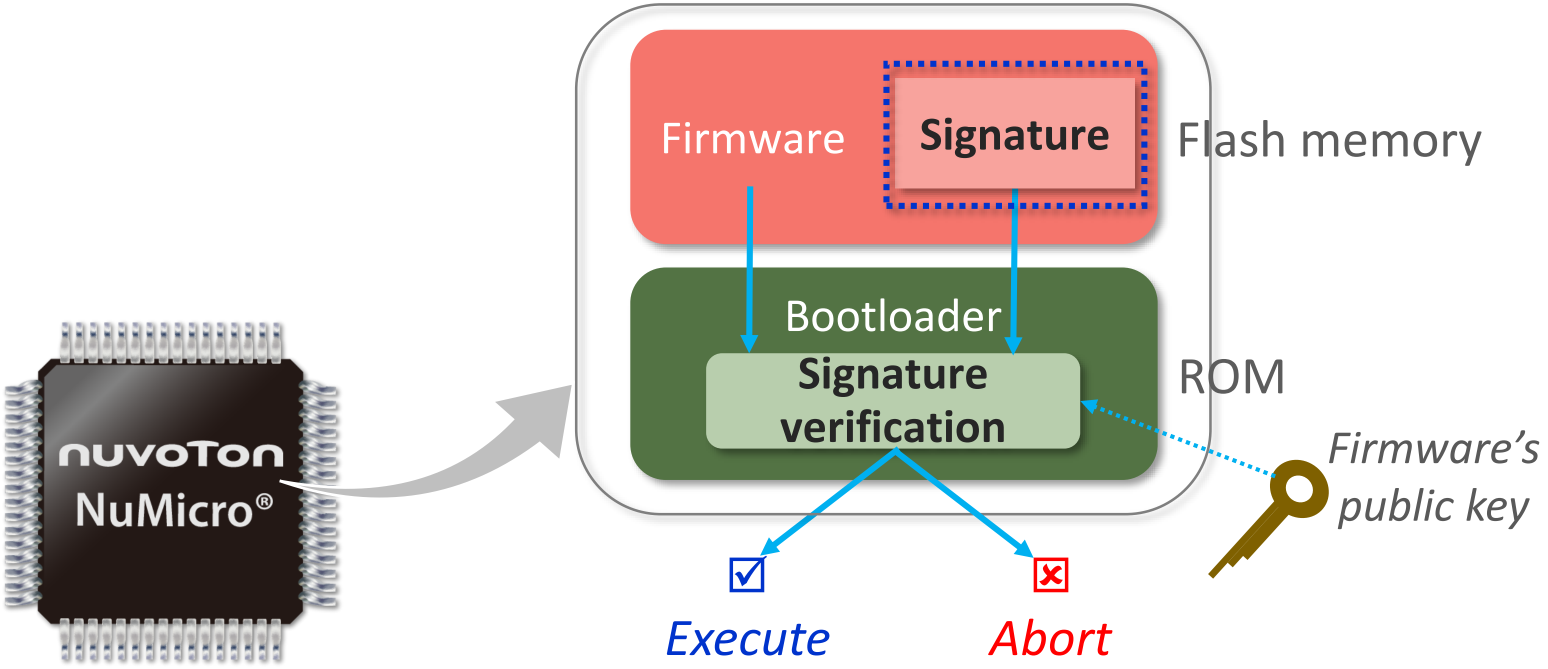
- MCU Security Technology


Unique ID / Debug Port Management
Tamper pins / Clock Monitor / Voltage sensor
Crypto Accelerator / TRNG / KeyStore
TrustZone / Memory Protection Unit
Secure Boot
Life cycle attack
Intrusion detection / FIA[*1]
Communication / SCA
Software attack

[*1] *FIA : Faut Injection Attack*

MCU Security Features

- **Secure Boot**
  - Hardware Root of Trust
    - An immutable ROM code cryptographically verifies firmware's **Integrity** and **Authenticity** after system power-on or reset

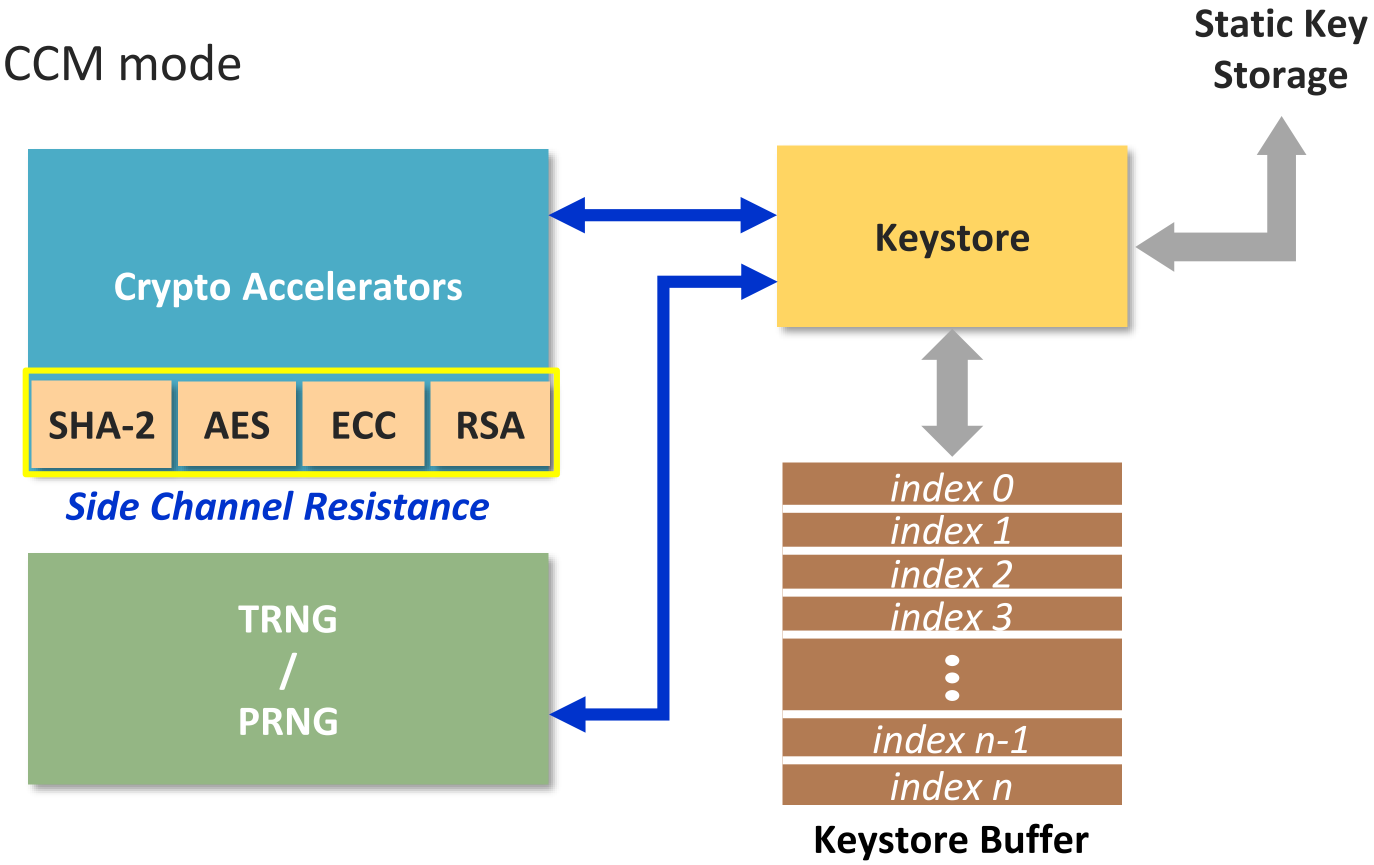


MCU Security Features

- **Unique Identifier (UID)**
  - A unique identifier used to identify an individual MCU
    - Device authentication
    - Derive encryption keys
  - Type of UID
    - 96-bit or 128-bit number decided during manufacturing stage

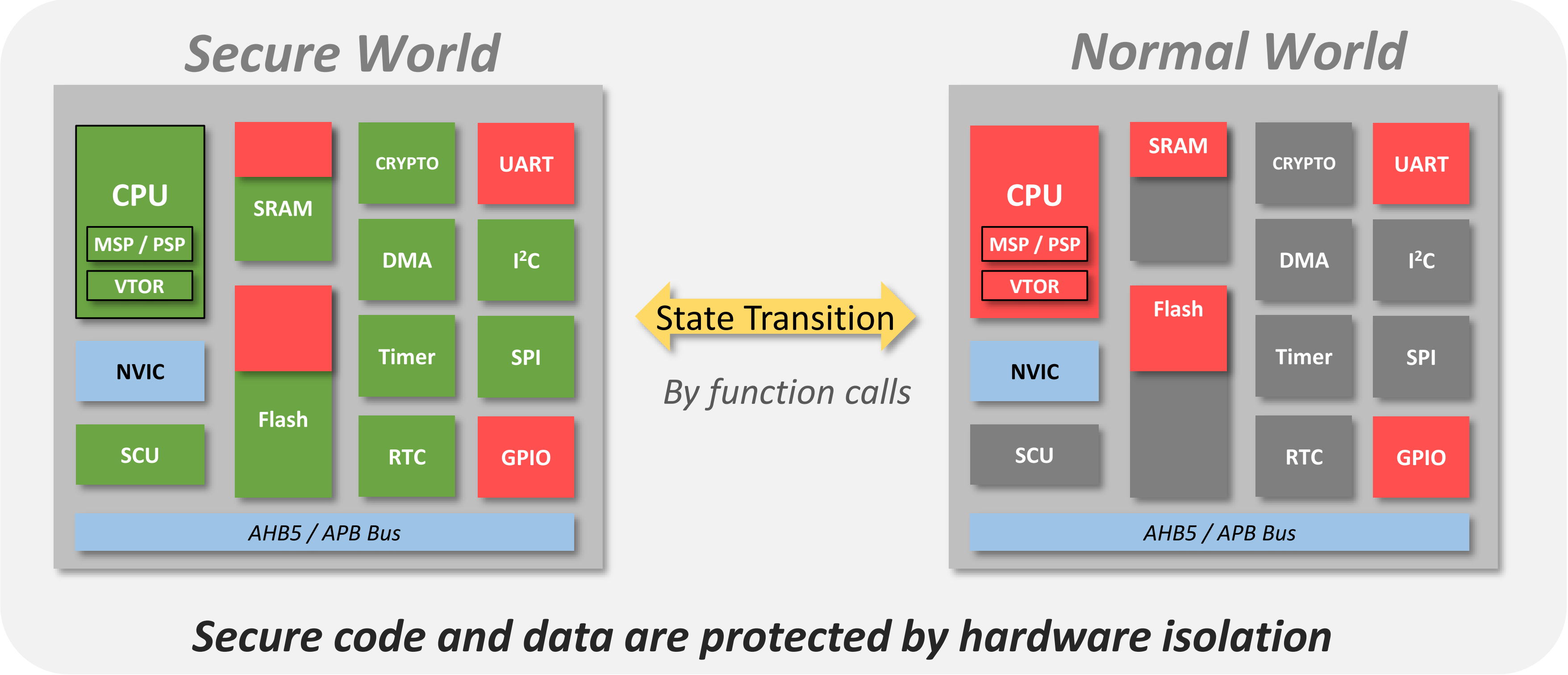
MCU Security Features

- **Hardware Crypto Accelerators**
  - Data Encryption / Decryption
    - AES-128 / AES-256 / GCM mode, CCM mode
  - Data Integrity Check
    - SHA-256 / SHA-512
  - Signature Verification
    - ECDSA
    - RSA
  - Key Exchange
    - ECDH
  - True Random Number



MCU Security Features

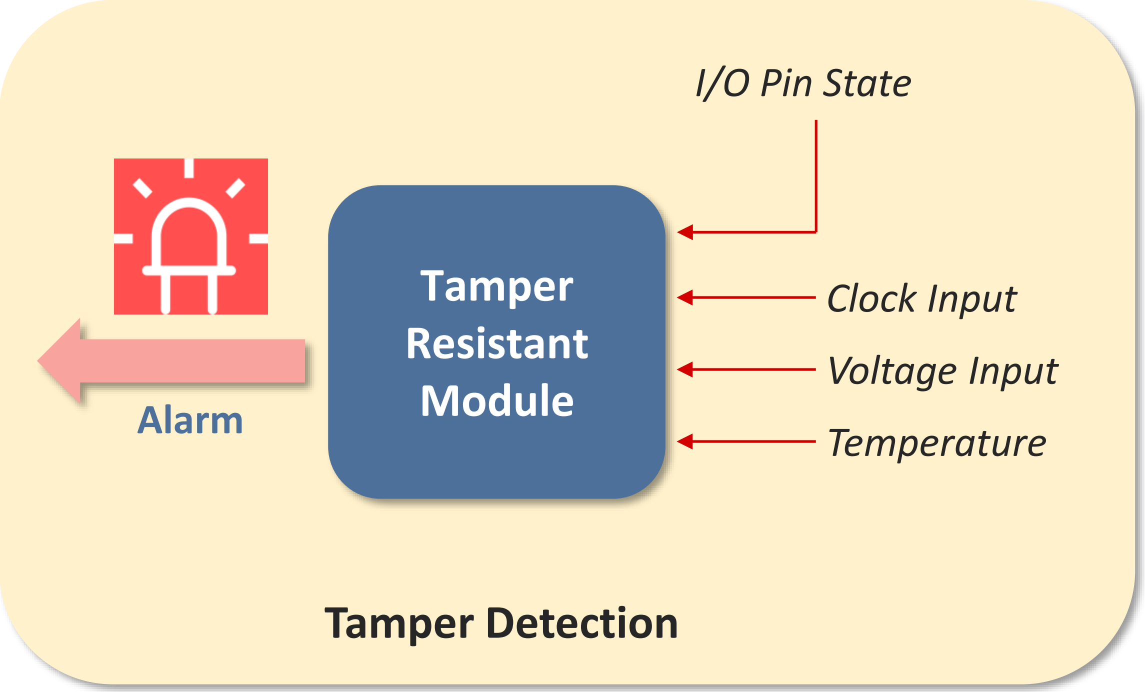
- **TrustZone**
  - TrustZone partitions the system into **Secure** (Trusted) and **Normal** (Non-trusted) worlds according to **memory address**.



Secure code and data are protected by hardware isolation

MCU Security Features

- **Tamper Resistant Module**
  - Detect abnormal situation and take adapted action
    - Tamper events
      - Incorrect pin state (case-open event)
      - Clock : glitch, out of range
      - Voltage : glitch, over/under voltage
      - Temperature : out of range
    - Adapted action
      - Tamper event interrupts
      - Clear backup SRAM or registers



Conclusions

Protecting the data integrity and authenticity of IoT devices is the foundation of IoT security.

MCUs should have hardware security features to defend against software attacks, side-channel attacks, and fault injection attacks.

Joy of innovation

nuvoTon

谢谢

謝謝

Děkuji

Bedankt

Thank you

Kiitos

Merci

Danke

Grazie

ありがとう

감사합니다

Dziękujemy

Obrigado

Спасибо

Gracias

Teşekkür ederim

Cảm ơn