

# IoT Security Solutions

## Security Technologies

凌立民 Robert Ling

Microcontroller Application Business Group

Senior Technology Manager



# | Common IoT Security Threats (1)

- Unsafe communication, unauthorized access

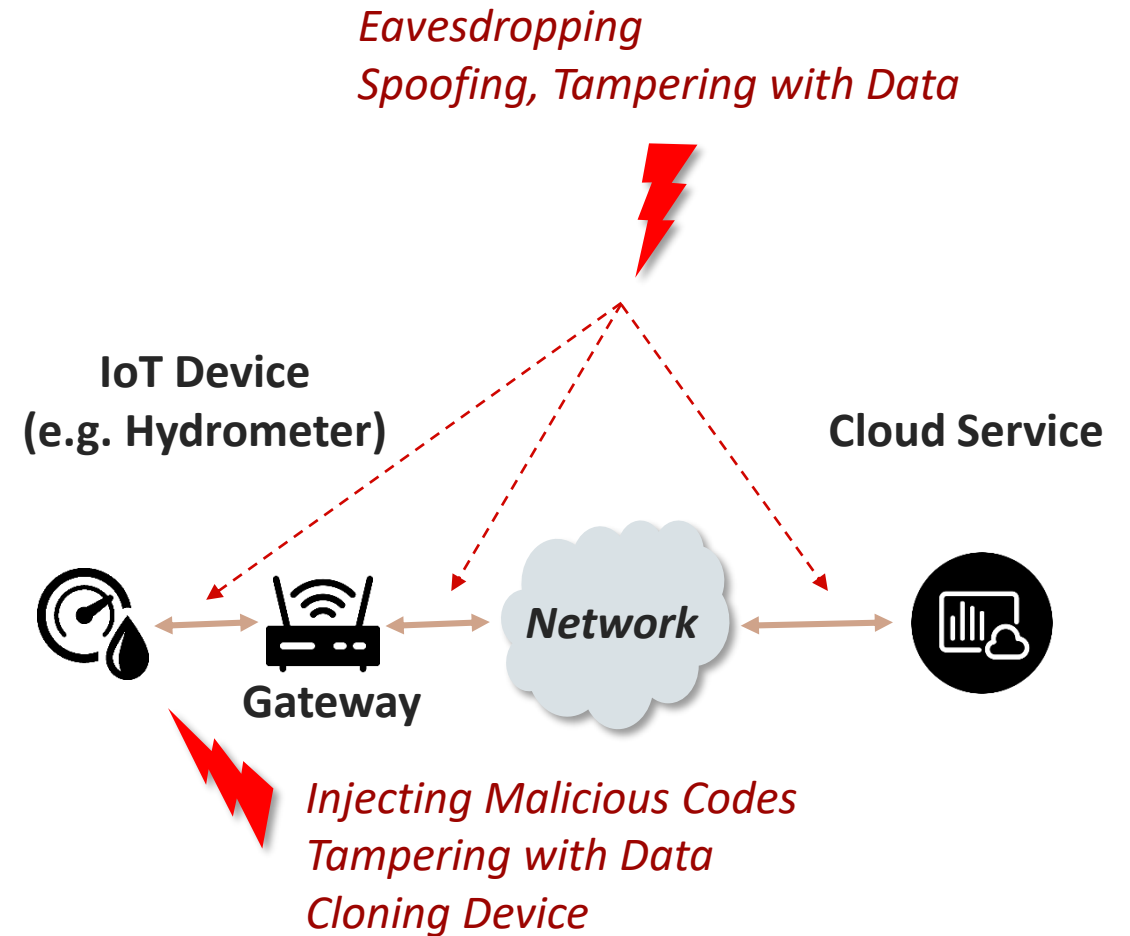
Remote Access, private Information Leaks,  
home Invasions, .....

## How do we protect the connection?

- Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocol
- Digital certificates
- Symmetric and asymmetric key system, authentication

## Security blocks from MCU

- Secure storage for unique ID, certifications, keys, etc.
- Unpredictable random number generator
- Cryptographic Accelerator: ECC, AES, DES/3DES, ...



# | Common IoT Security Threats (2)

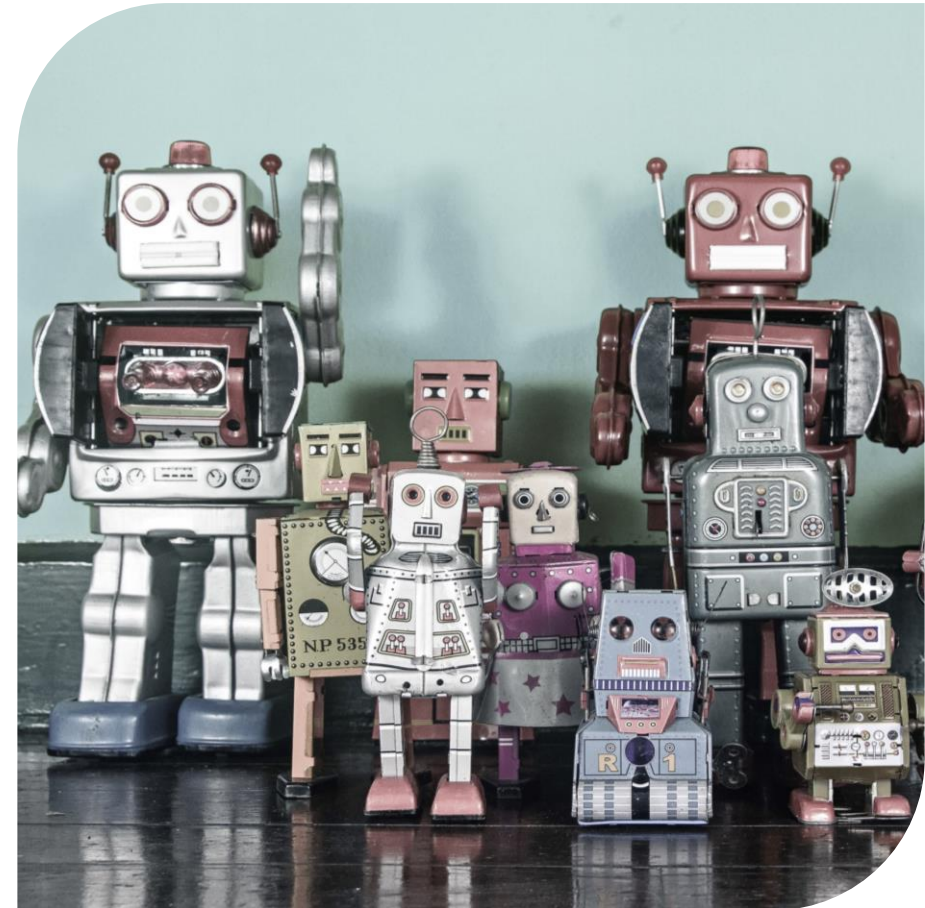
- Unsafe communication or access
- **Compromised IoT devices**

Botnet attack, malware attack, ...

How do we authorize the embedded firmware image and firmware update?

Security building blocks from MCU

- Secure boot and secure OTA
- Secure storage for certifications, keys, signature, etc.
- Cryptographic Accelerator: ECC, SHA, and HMAC-SHA
- Trust Zone to limit access
- OTP for life cycle management





# | Common IoT Security Threats (3)

- Unsafe communication or access
- Compromised IoT devices
- **Physical attack**

**Physical tampering, JTAG access, clocking**

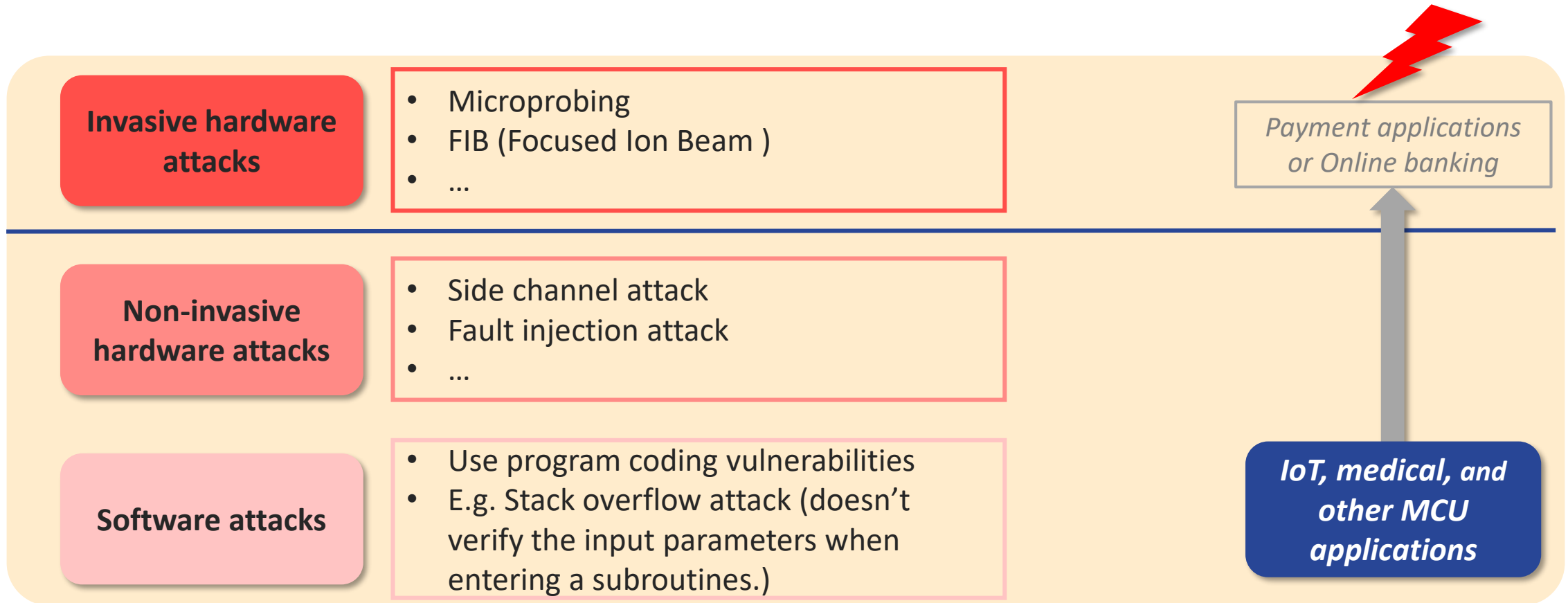
## **Security building blocks from MCU**

- Physical tempering detection
- Protected flash memory
- Trust Zone to limit access
- Clock monitoring and voltage glitch detection



# | MCU Security Target

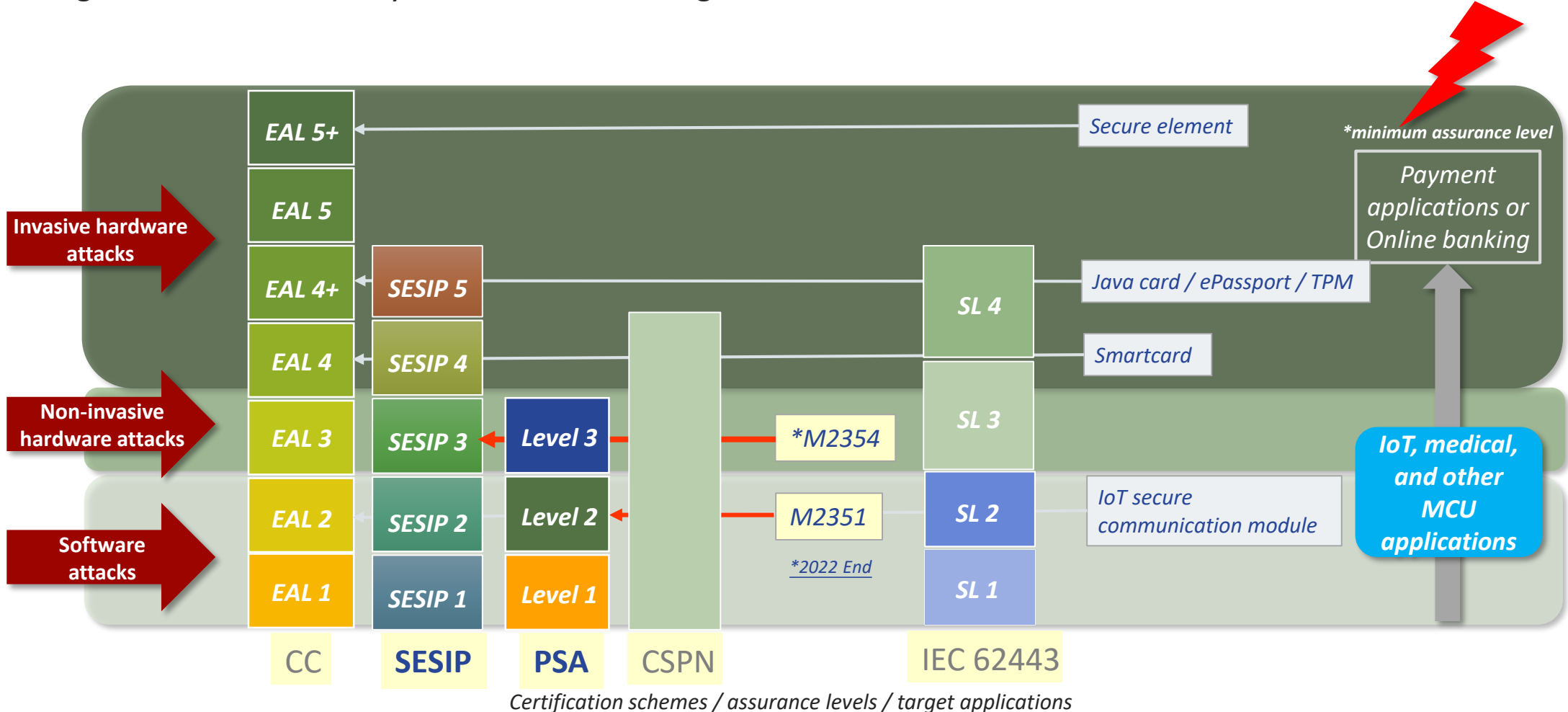
- Implement the security features to defend against **software attacks** and **non-invasive hardware attacks**.



**Attacks types on MCU**

# Current Progress of IoT Security Related Certifications

- Integrate sufficient security features to defend against **software attacks** and **non-invasive hardware attacks**.



# M235x Security Features at a Glance

*Device & Customer identification (UID, CID)*

*Integrity check and secure firmware upgrade*

*Hardware authentication for updating Flash memory*

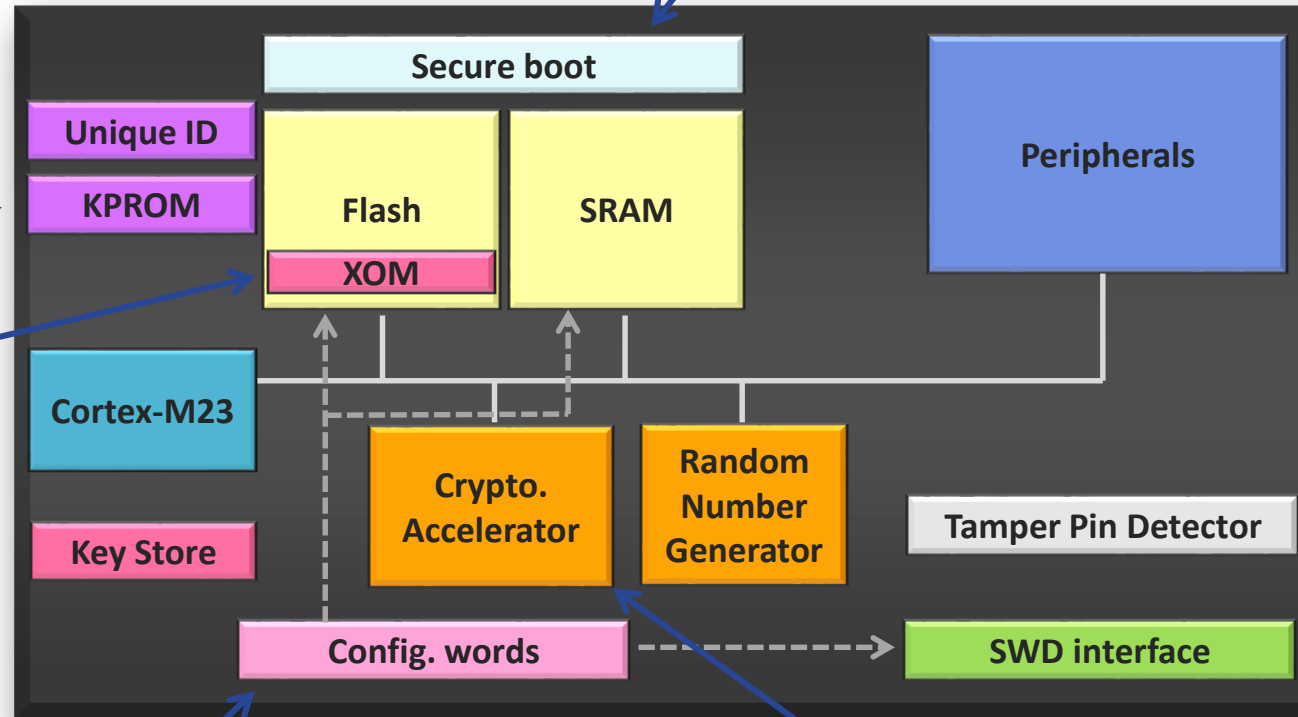
*eXecute-Only Memory region for SW IP protection*

*TrustZone Isolation, Voltage and Clock glitches detection and protection*

**Chip-Level Active Shield (M2354)**

*Multiple level setting for Flash lock, SWD disabled for Secure Debug*

**Countermeasures to Side-Channel Monitoring for encryption and decryption operations (M2354)**



*Detect input state transition*

*Secure Debug Interface and Function*

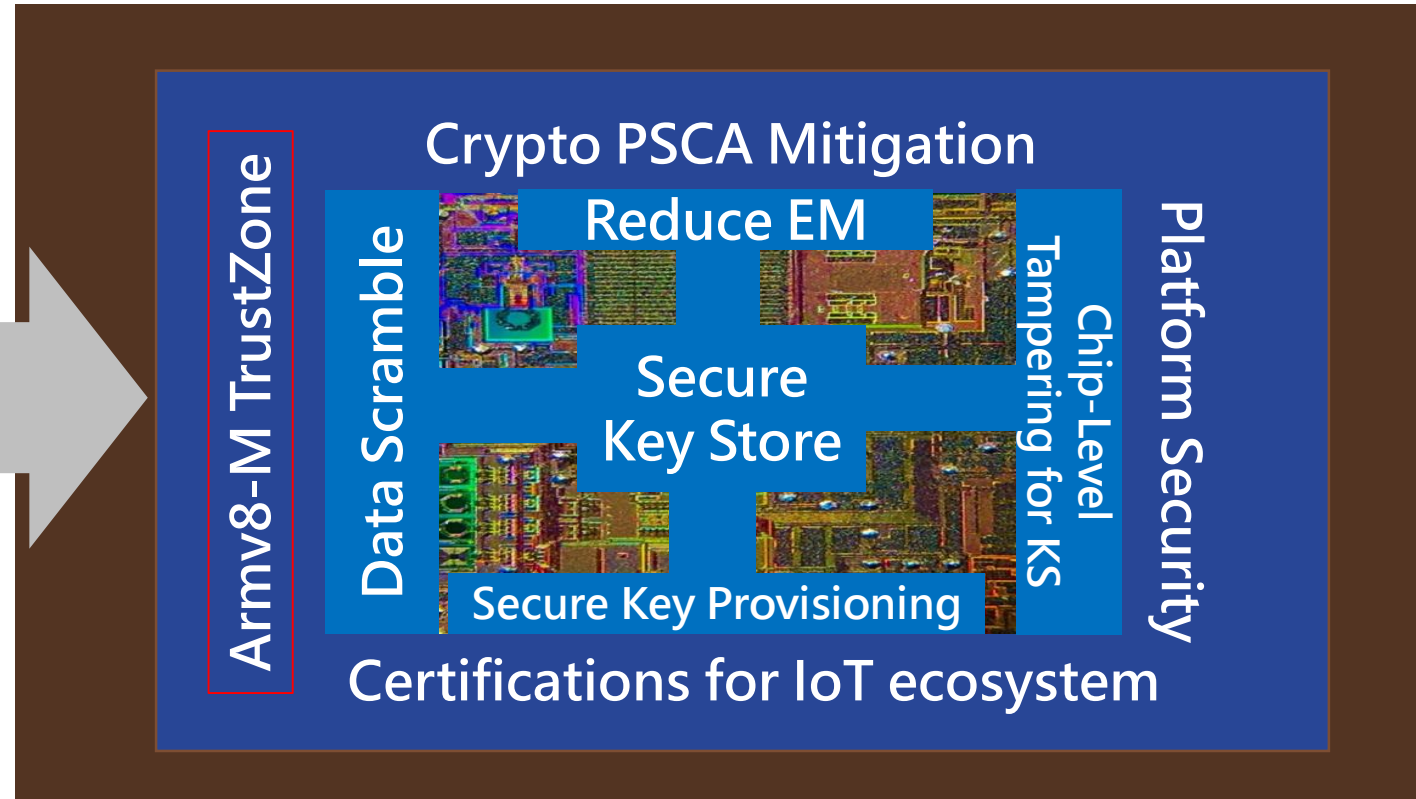
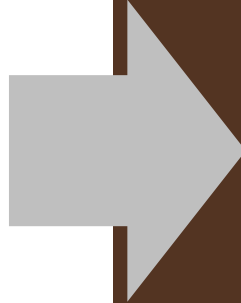
# | M235x IoT Security Microcontroller

M2351

TZ-CPU (SW RoT) + Crypto +  
PCB Tampering

M2354

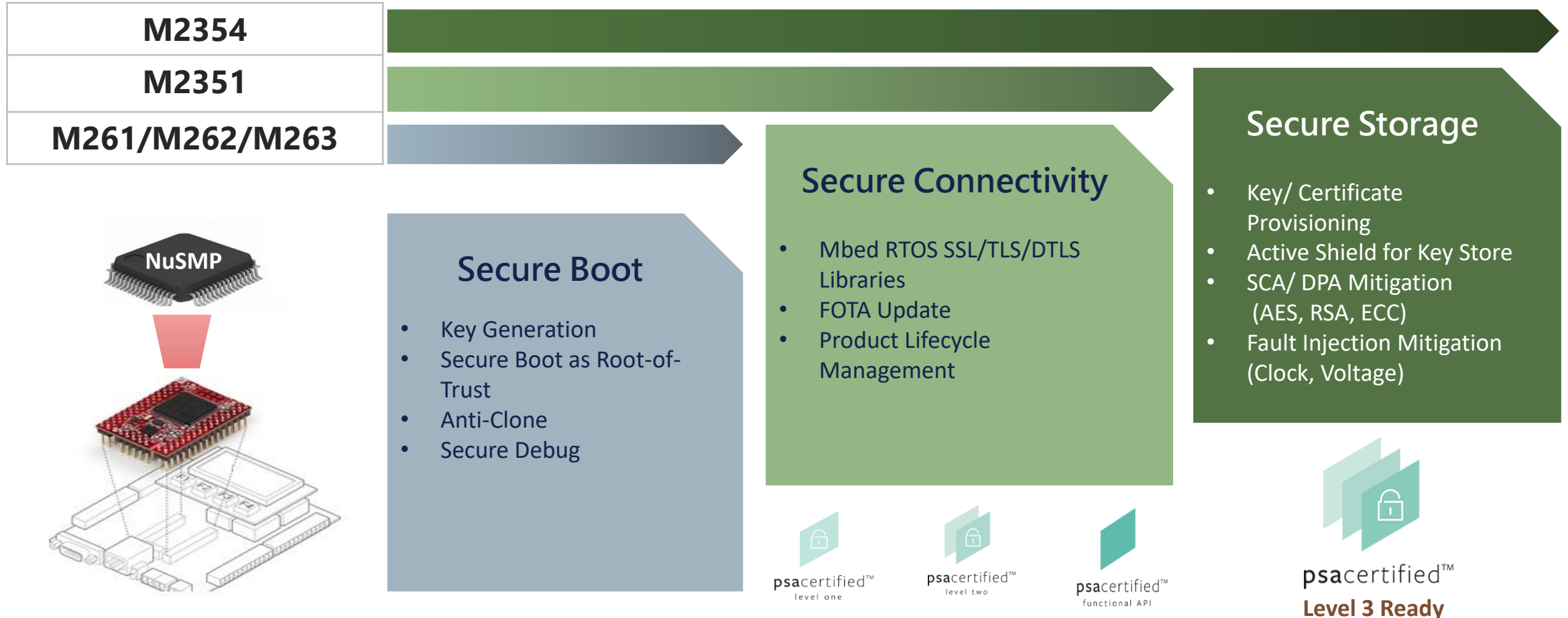
TZ-CPU + HW RoT (KS) + Crypto with PSCA  
mitigation + Platform Security + Certification



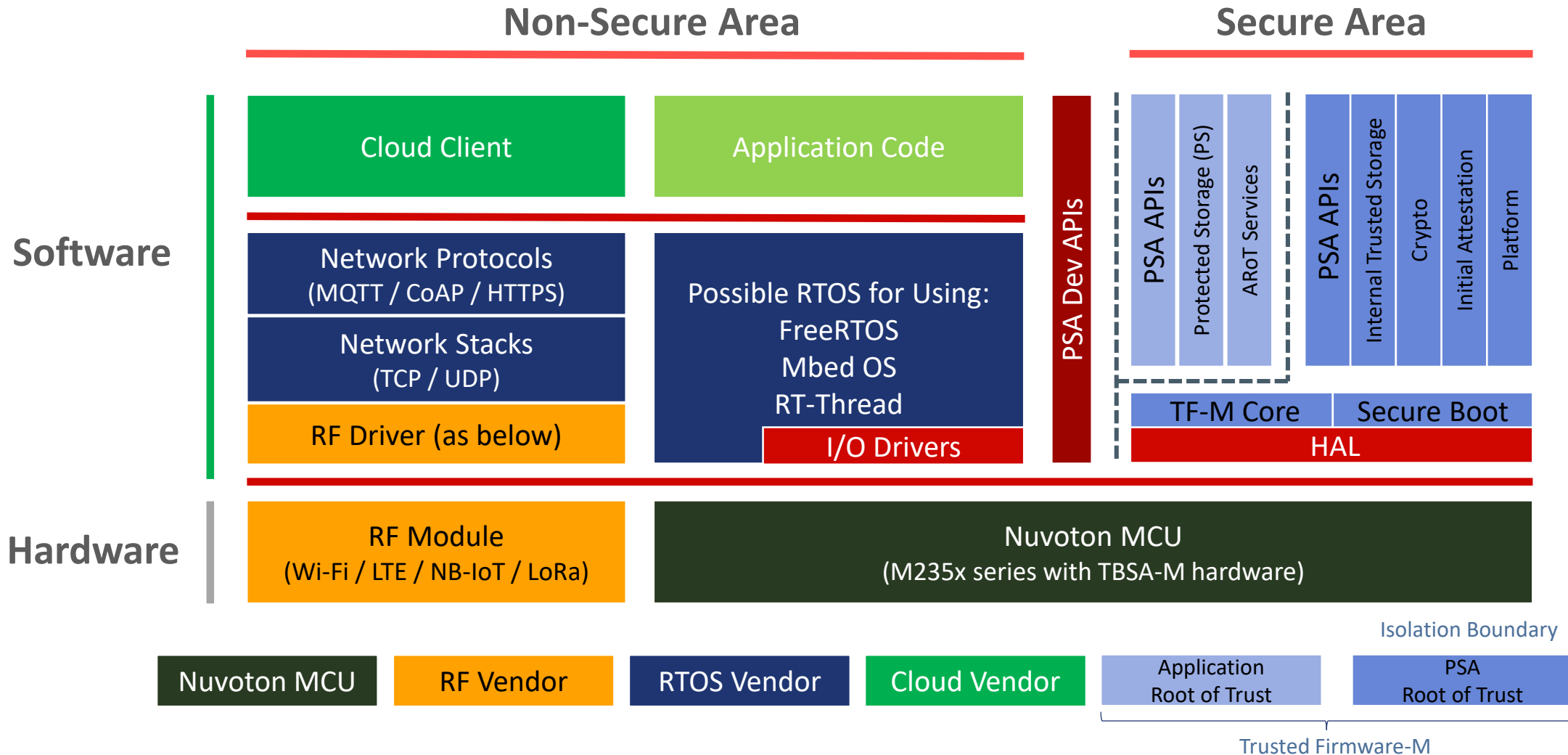


# | Main Security Features of NuMicro<sup>®</sup> M235x

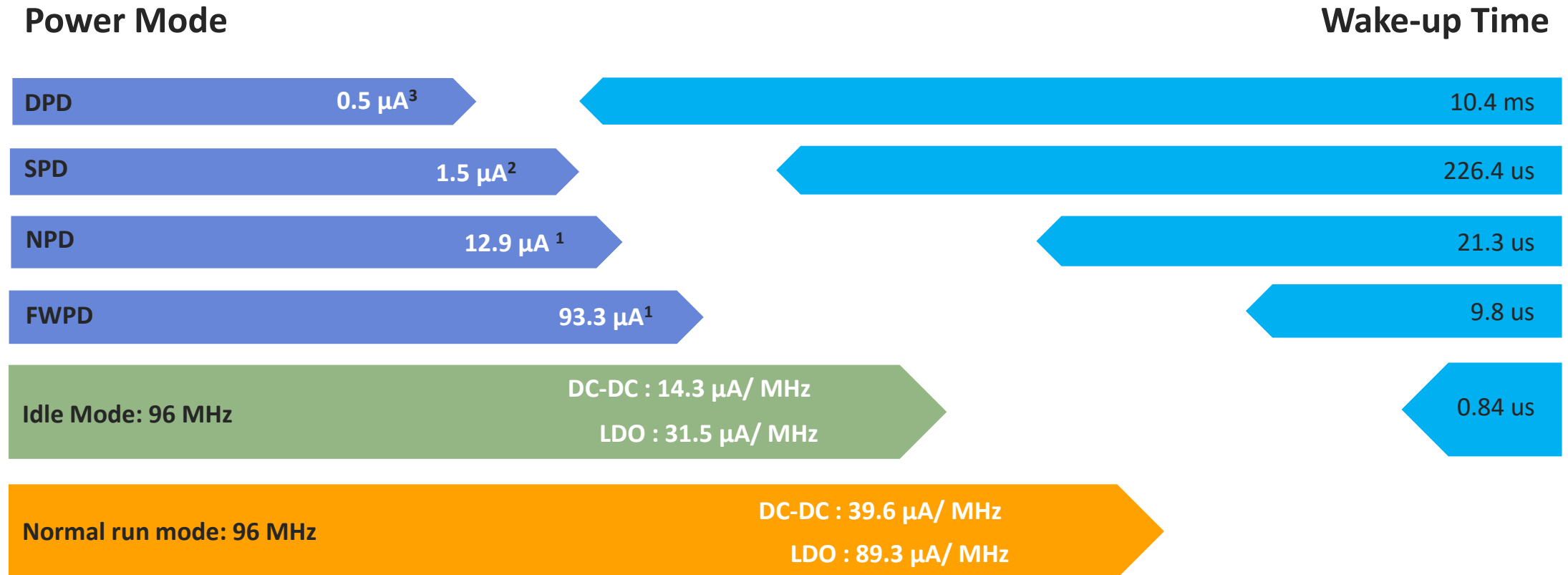
- NuMicro<sup>®</sup> Secure Microcontroller Platform: Secure Boot, Secure Connectivity, Secure Storage (**NuSMP**).



# M2354 IoT Platform with TF-M (Q4, 2022)



# M2354 Series Power Performance



Note: 1. Keep all SRAM retention  
2. Only keep 4 KB SRAM retention  
3. With RTC register 80 bytes retention

# | Support Multiple Real-Time Operating Systems

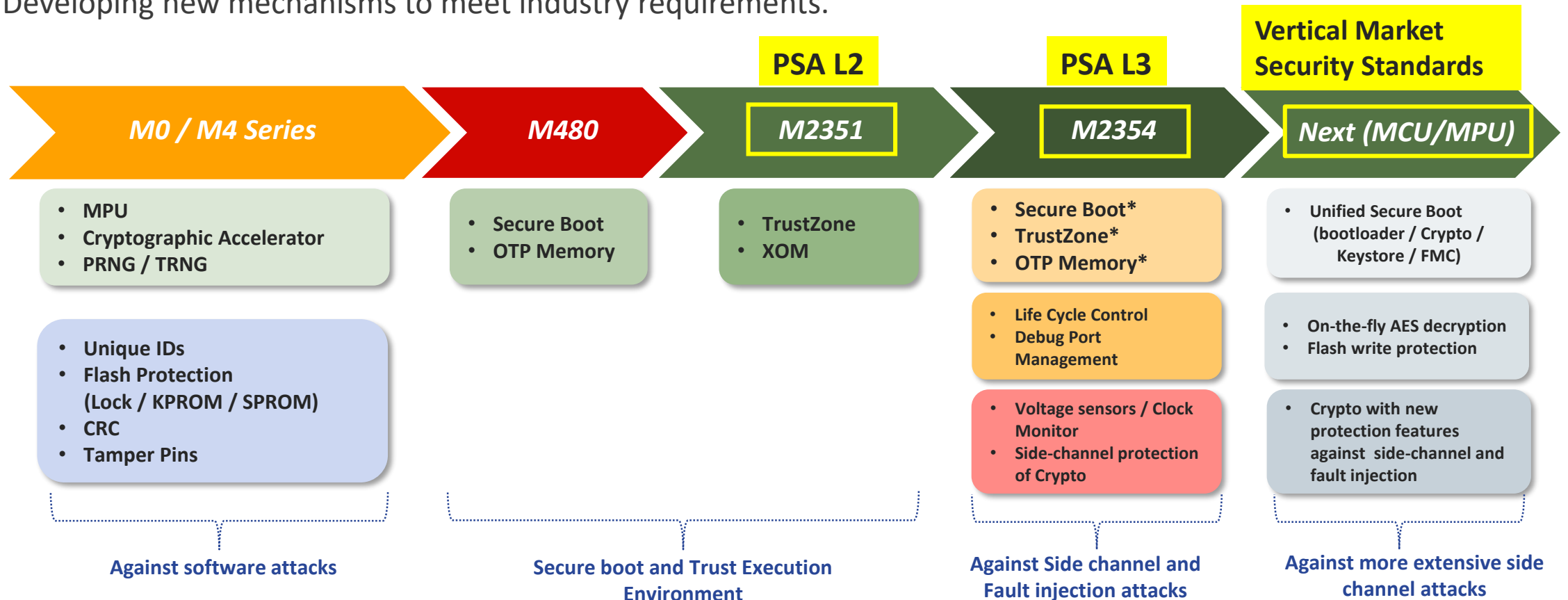
- Speed up your RTOS porting - OS ready solution to save your OS porting time.

Core	NuMaker Boards/ NK + Extension Boards	IP Connectivity Ready				Support RTOS			Support Cloud		
		Wi-Fi	NB-IoT	802.15.4 Thread + ZigBee	LoRa (915 MHz, 470 MHz)	Mbed OS	FreeRTOS	RT-Thread	Arm Pelion Device Manager	Amazon AWS IoT	Microsoft Azure IoT Hub
Cortex-M23	NK-BEDM2351 (w/ 802.15.4 module)	●		●		●	●	●	●	●	●
	NuMaker-IoT-M263A	●	●			●	●	●	●	●	●
	NK-BEDM2354	●				●	●	●	●	●	●
	NuMaker-IoT-M2354	●		●	●	●	●	●	●	●	●



# Nuvoton Security Technology Roadmap

- Able to against **software attacks** and **lightweight hardware attacks** as well as provide **Secure boot** and **Trust Execution Environment**.
- Developing new mechanisms to meet industry requirements.





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

# | NuMicro<sup>®</sup> IoT Security Technology Summary

## MCU System Security



### Secure Boot

Secure Bootloader in ROM with Driver APIs



### Device Identification

Unique ID, Customer Unique ID



### Isolation

TrustZone-M, TrustZone-A, Peripheral Privileged Mode, Trusted Secure Island (TSI for MPU)



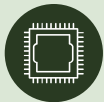
### Flash Memory Protection

Read/Write Protection, eExecute-Only Memory (XOM), Dual-Bank with Bank Swap



### System Anti-Tampering

Tamper Detection Pins, RTC Domain Backup Registers



### Chip-Level Security

Temperature Sensor, Clock Function Monitor, Voltage Glitch Detection

## Crypto Security



### TRNG, Hardware Accelerators, Secure Storage

TRNG, DES/3DES, SHA, AES, RSA, ECC, Power Side-Channel Attack Mitigation for AES/RSA/ECC, Secure Key-Store, China SM2/SM3/SM4

## Product Lifecycle Security



### Product Lifecycle Management

Booting Status Monitor, Lifecycle Management, Firmware Version Counter



### Secure Debug

Debug Authentication (temporarily unlock), Debug Port Management (DPM)

## Software and Service



### Security Reference Software and Provisioning

Key Generation Tool, Firmware Image Signing Tool, OTA Update, Key/Certificate Provisioning Service