IoT Security Solutions

An Introduction to IoT Security Products of NuMicro® Family

Robert Ling

Microcontroller Application Business Group

Senior Technology Manager

| Photo by Jeffery Cheng

Common IoT Security Threats (1)

- **Unsafe communication, unauthorized access**

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

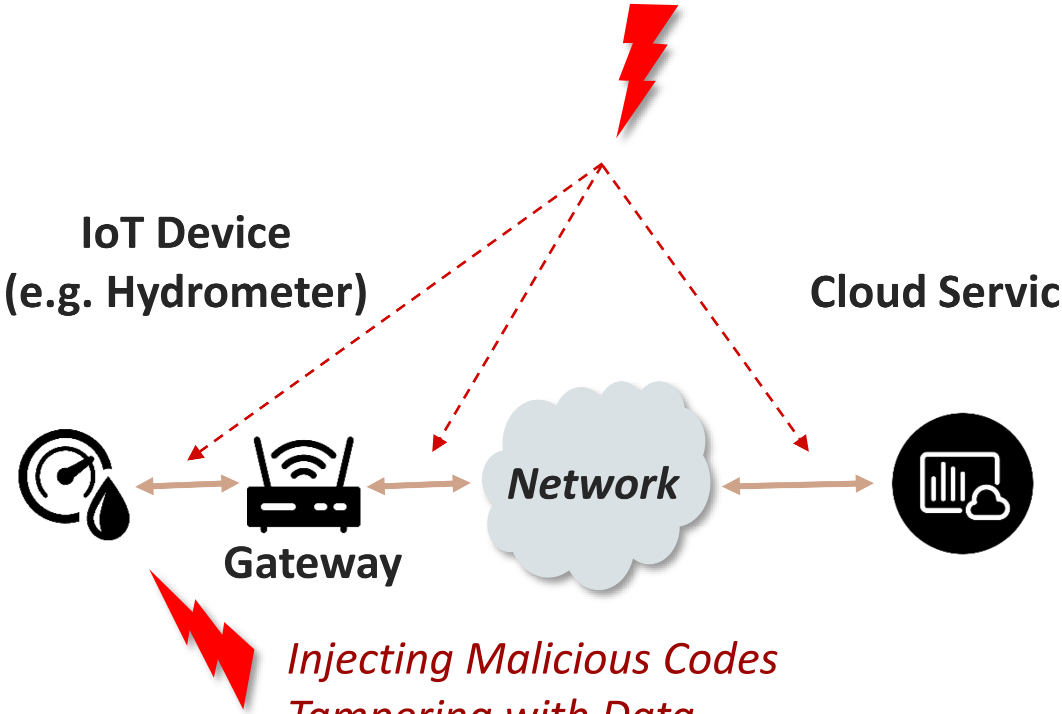
How do we protect the connection?

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

Security features of an MCU

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

Eavesdropping
Spoofing, Tampering with Data



Injecting Malicious Codes
Tampering with Data
Cloning Device

Common IoT Security Threats (2)

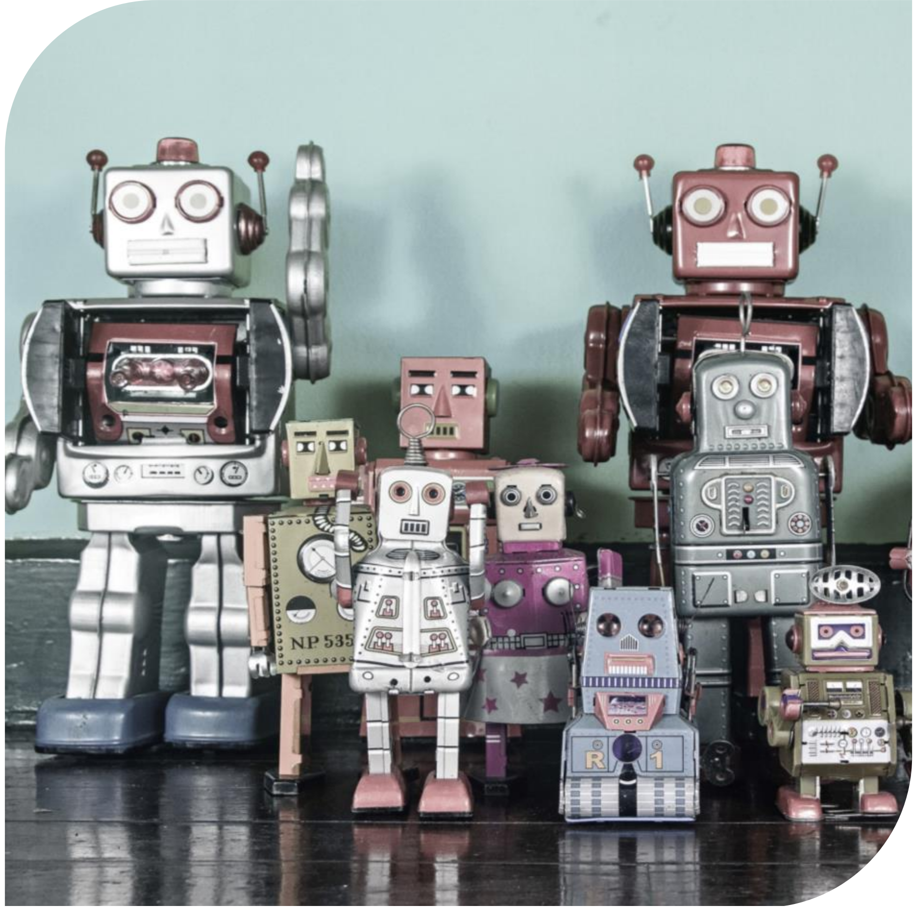
- Unsafe communication or access
- Compromised IoT devices

Botnet attack, malware attack, …

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

Security features of an MCU

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



Common IoT Security Threats (3)

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

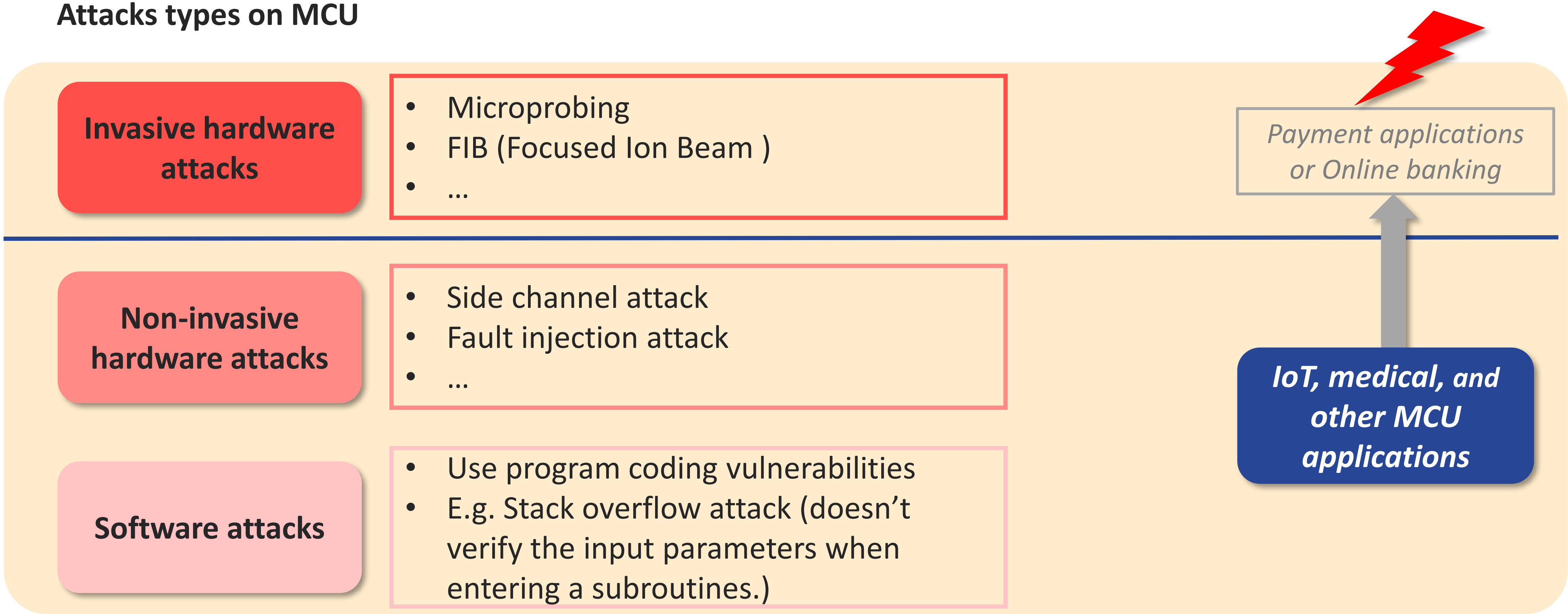
Physical tampering, JTAG access, clocking

Security features of an MCU

- Physical tempering detection
- Protected Flash memory
- TrustZone isolation to limit access
- Clock monitoring and voltage glitch detection

MCU Security Target

Attacks types on MCU



Invasive hardware attacks

- Microprobing
- FIB (Focused Ion Beam)
- …

Non-invasive hardware attacks

- Side channel attack
- Fault injection attack
- …

Software attacks

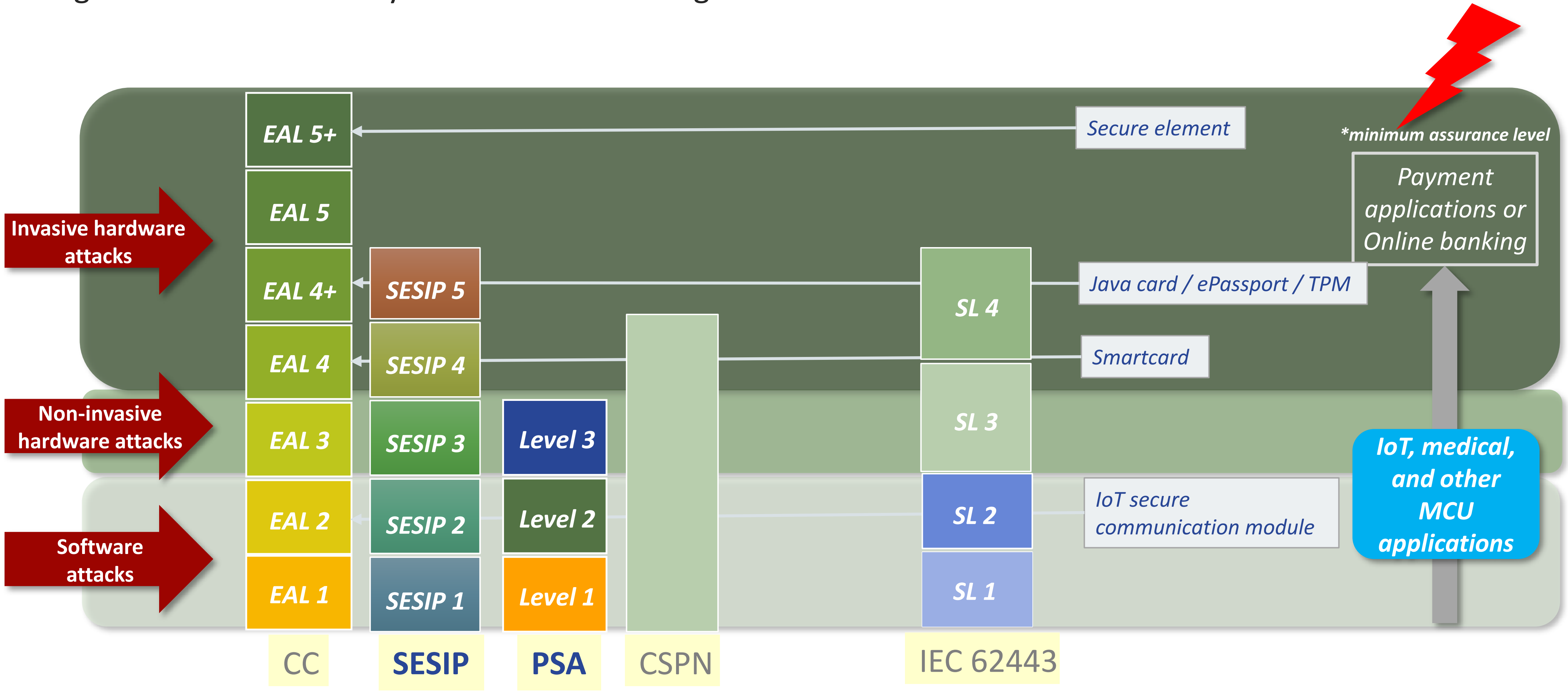
- Use program coding vulnerabilities
- E.g. Stack overflow attack (doesn’t verify the input parameters when entering a subroutines.)

Payment applications or Online banking

IoT, medical, and other MCU applications

Current Progress of IoT Security Related Certifications

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



Certification schemes / assurance levels / target applications

NuMicro® 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, eXecute-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

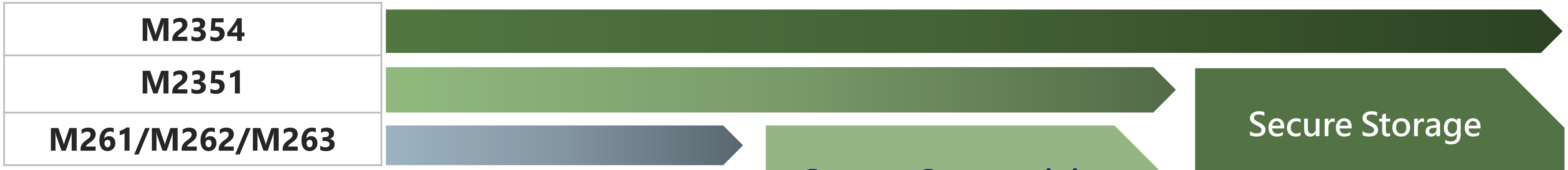
Product Lifecycle Management
Booting Status Monitor, Lifecycle Management, Firmware Version Counter

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

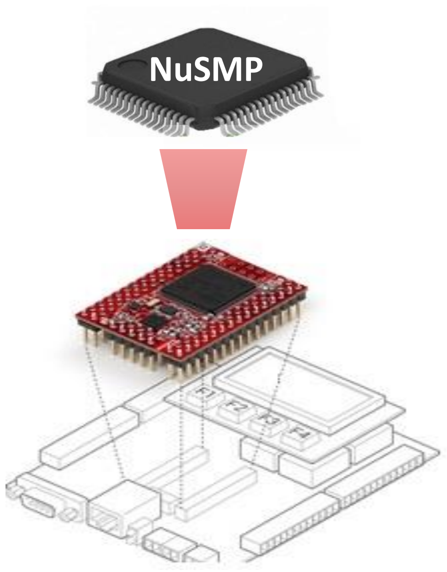
Software and Service

Security Reference Software and Provisioning
Key Generation Tool, Firmware Image Signing Tool, OTA Update, Key/Certificate Provisioning Service

Main Security Features of NuMicro® M235x



M2354
M2351
M261/M262/M263



Secure Boot

- Key Generation
- Secure Boot as Root-of-Trust
- Anti-Clone
- Secure Debug

Secure Connectivity

- Mbed RTOS SSL/TLS/DTLS Libraries
- FOTA Update
- Product Lifecycle Management

psacertified™ level one

psacertified™ level two

psacertified™ functional API

Secure Storage

- Key/ Certificate Provisioning
- Active Shield for Key Store
- SCA/ DPA Mitigation (AES, RSA, ECC)
- Fault Injection Mitigation (Clock, Voltage)

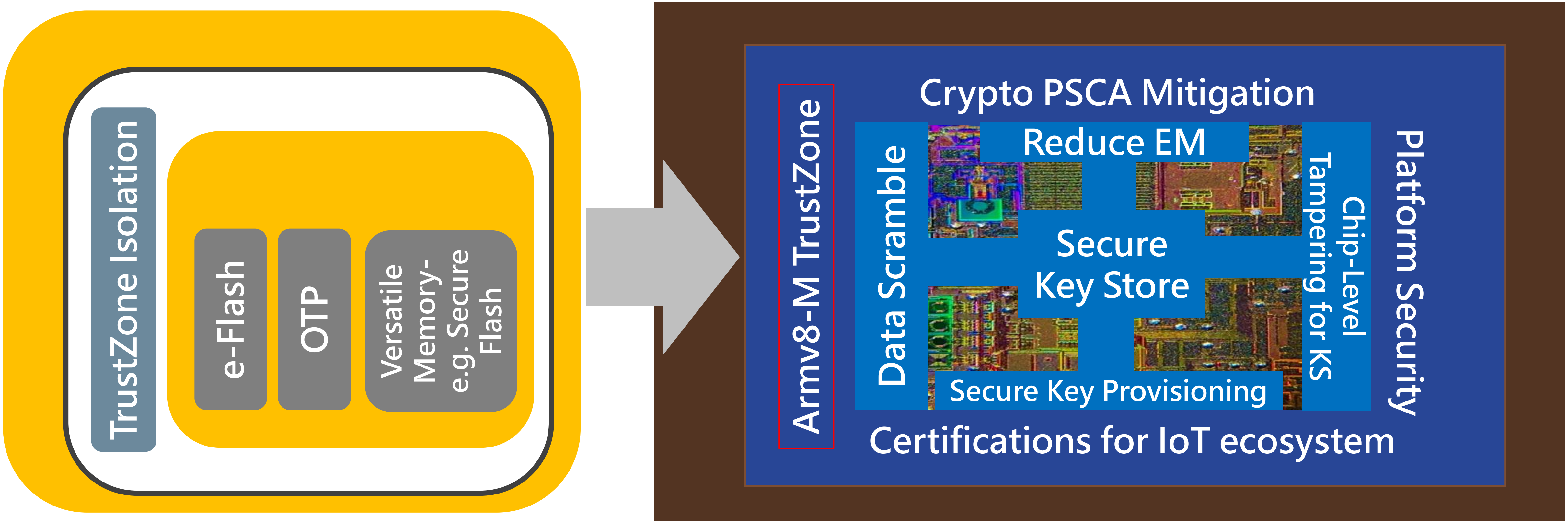
psacertified™

Level 3 Ready

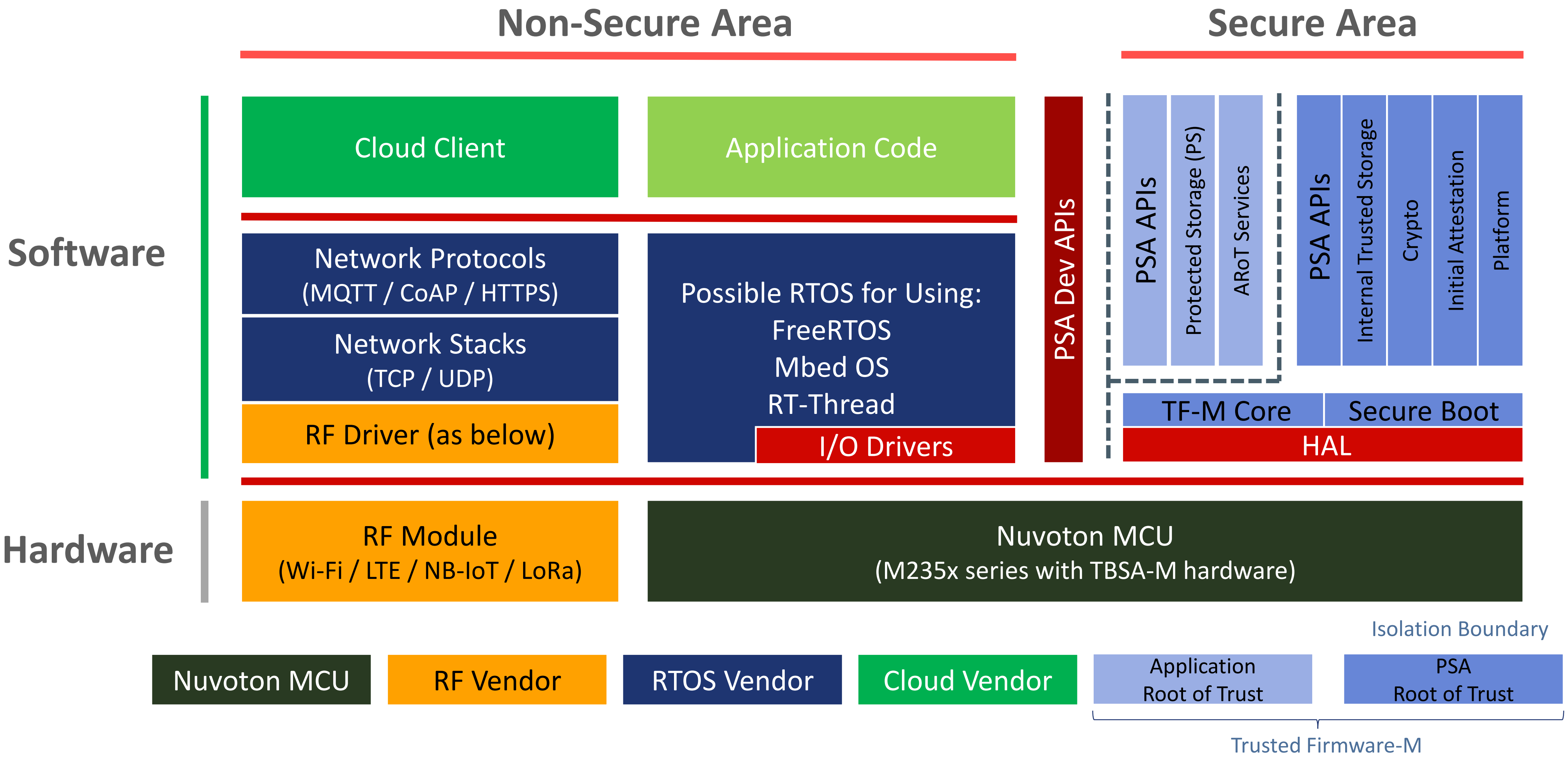
M235x IoT Security Microcontroller

M2351
TZ-CPU (SW RoT) + Crypto + PCB Tampering

M2354
TZ-CPU + HW RoT (KS) + Crypto with PSCA mitigation + Platform Security + Certification

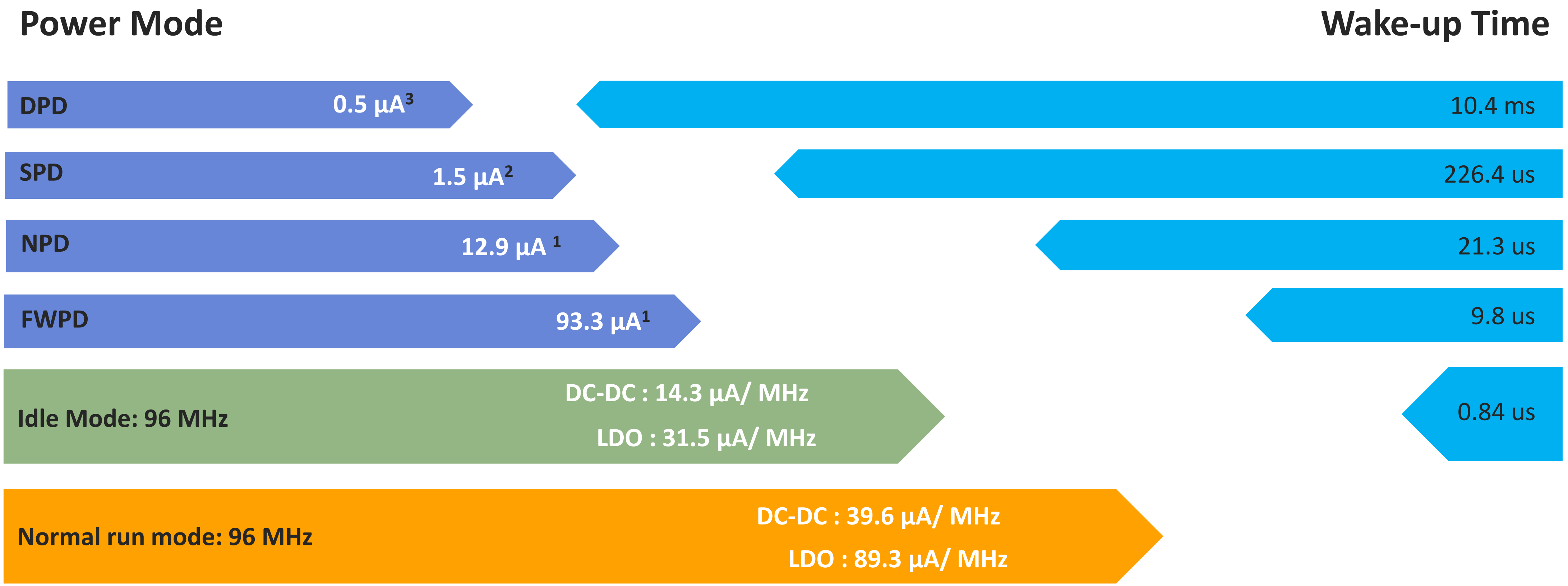


M2354 IoT Platform with TF-M



|

M2354 Series Power Performance



Power Mode

Wake-up Time

DPD 0.5 µA[3] — 10.4 ms

SPD 1.5 µA[2] — 226.4 us

NPD 12.9 µA [1] — 21.3 us

FWPD 93.3 µA[1] — 9.8 us

Idle Mode: 96 MHz
DC-DC : 14.3 µA/ MHz
LDO : 31.5 µA/ MHz
— 0.84 us

Normal run mode: 96 MHz
DC-DC : 39.6 µA/ MHz
LDO : 89.3 µA/ MHz

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	●		●	●	●	●	●	●	●	●

Advanced Security Features for Cyber Security

- **The MA35D1 is a trusted system for IoT products' security requirements.**

Execution Security

TrustZone, Secure boot, Run-Time Integrity Checker (RTIC)

Communication Security

Hardware cryptographic accelerators

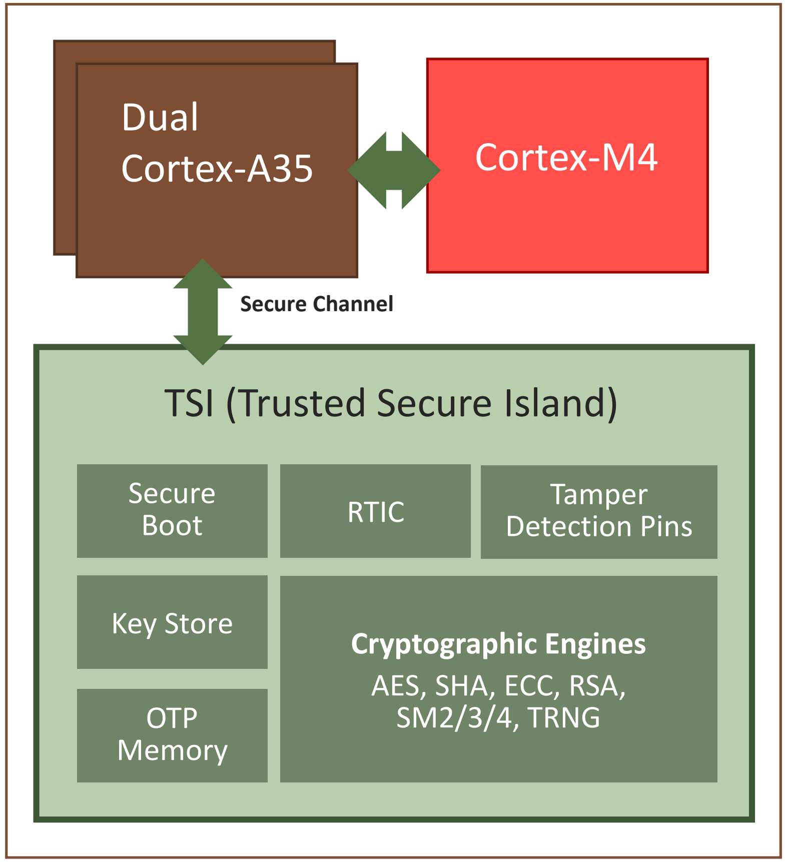
Chip-level Storage Security

Key Store and OTP memory, accessed by the cryptographic engines, without the need of CPU access

System Security

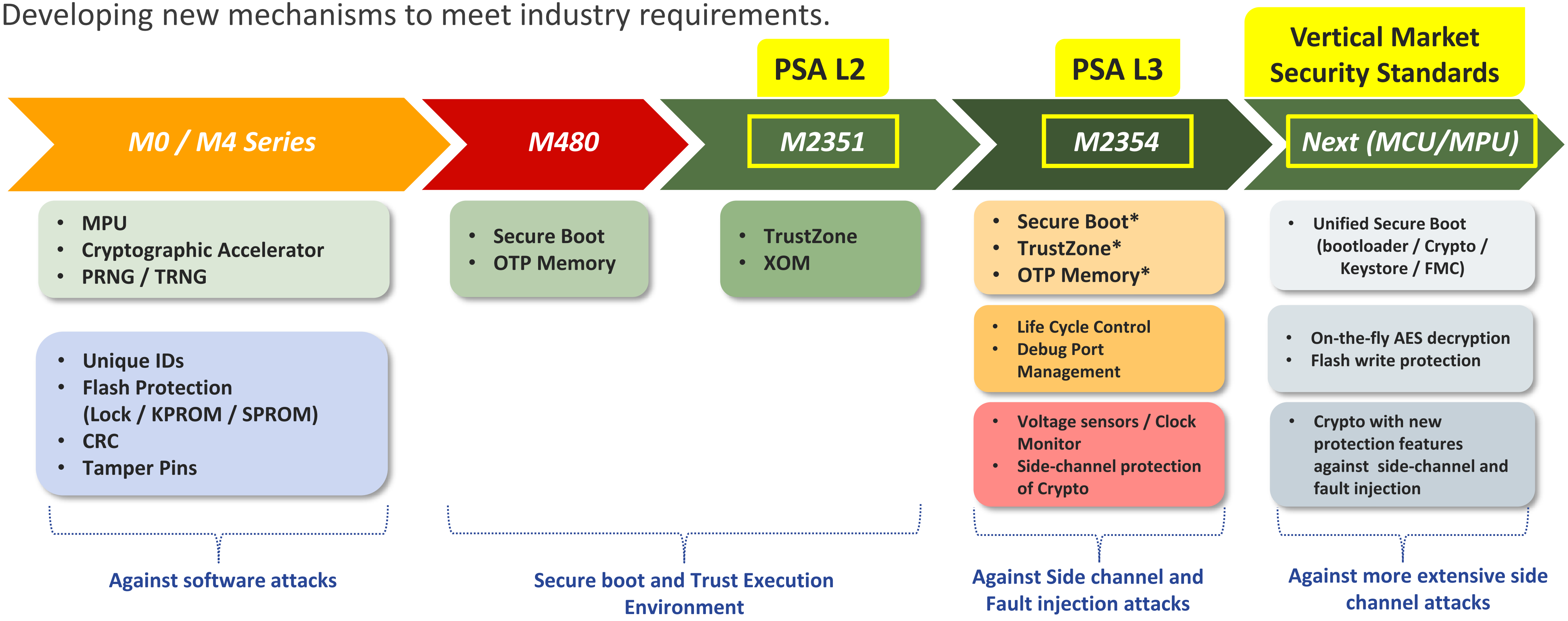
Tamper pins for tamper detection

- The secure environment and features realize the **Protection**, **Detection**, and **Recovery** for IoT products.
- The **Nuvoton Trusted Secure Island (TSI)** is an isolated secure hardware unit.
- Built-in cryptographic accelerators, Key Store, and OTP memory.
- Performs all the security operations, including secure boot and tamper pins detection.



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.



PSA L2

PSA L3

Vertical Market Security Standards

M0 / M4 Series

- MPU
- Cryptographic Accelerator
- PRNG / TRNG

- Unique IDs
- Flash Protection (Lock / KPROM / SPROM)
- CRC
- Tamper Pins

M480

- Secure Boot
- OTP Memory

M2351

- TrustZone
- XOM

M2354

- Secure Boot*
- TrustZone*
- OTP Memory*

- Life Cycle Control
- Debug Port Management

- Voltage sensors / Clock Monitor
- Side-channel protection of Crypto

Next (MCU/MPU)

- Unified Secure Boot (bootloader / Crypto / Keystore / FMC)

- On-the-fly AES decryption
- Flash write protection

- Crypto with new protection features against side-channel and fault injection

Against software attacks

Secure boot and Trust Execution Environment

Against Side channel and Fault injection attacks

Against more extensive side channel 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