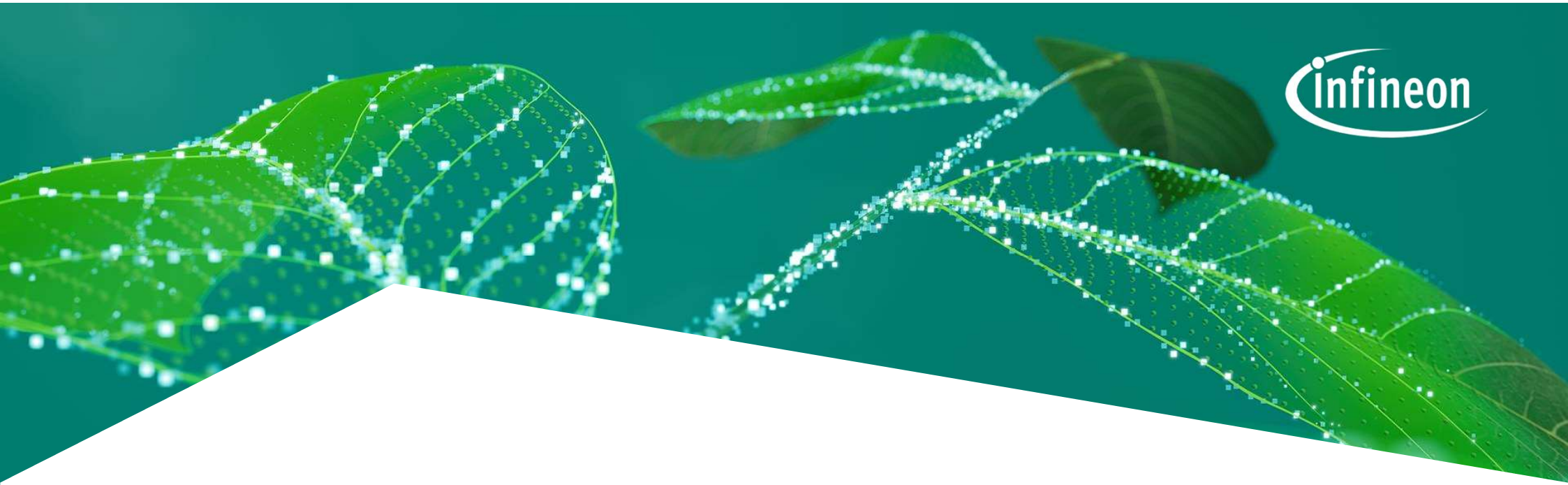


Security Challenges in Cyber-Physical Systems

Thomas Pöppelmann, Infineon Technologies

CPS Summer School 2024

Table of contents

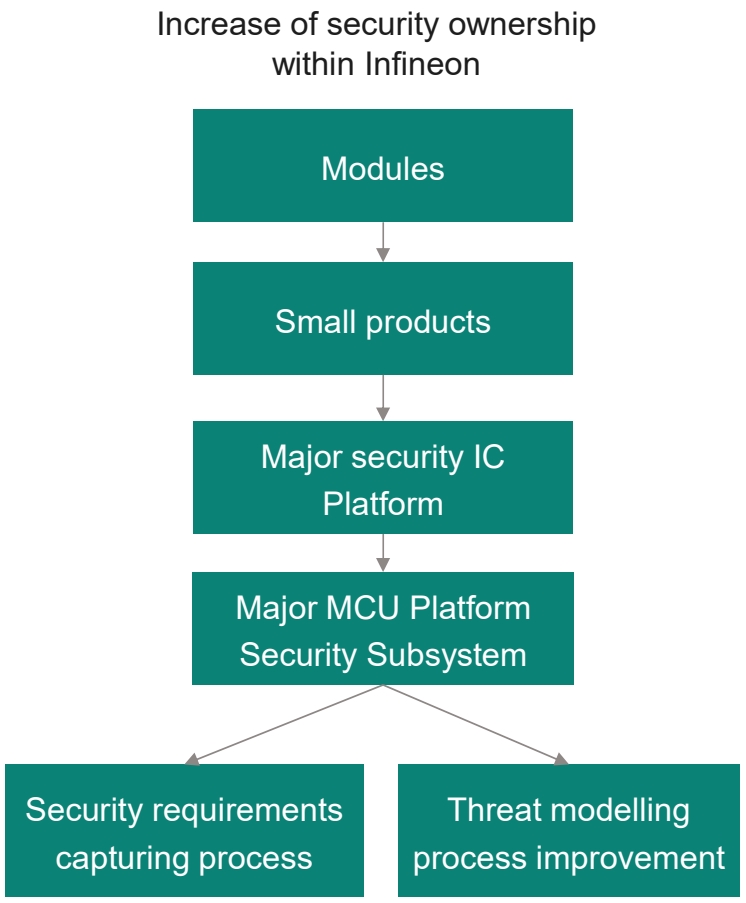
Introduction and content

- Goal of my presentation
  - Review generic security challenges in CPS
  - Show how security is layered in MCUs used to build CPS
  - Discuss some practical challenges and opportunities for further research

- Approach
  - Feel free to ask questions at any time

Self-introduction: From a PhD in PQC to security architecture

- Education
  - Studied Security in Information Technology at Ruhr-University Bochum
  - PhD at Ruhr-University Bochum on post-quantum cryptography (PQC) in 2015
- Started at Infineon in 2015
  - Infineon occupation: Concept engineering
  - One-year short term assignment (STA) in San Jose (2022 - 2023)
  - Now head of the Security Innovation team in the Digital Security & Identity (DSI) business line



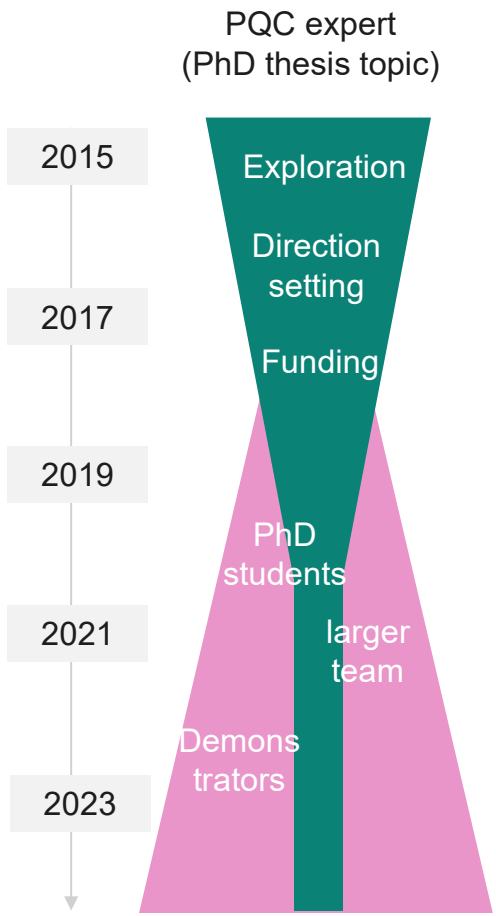
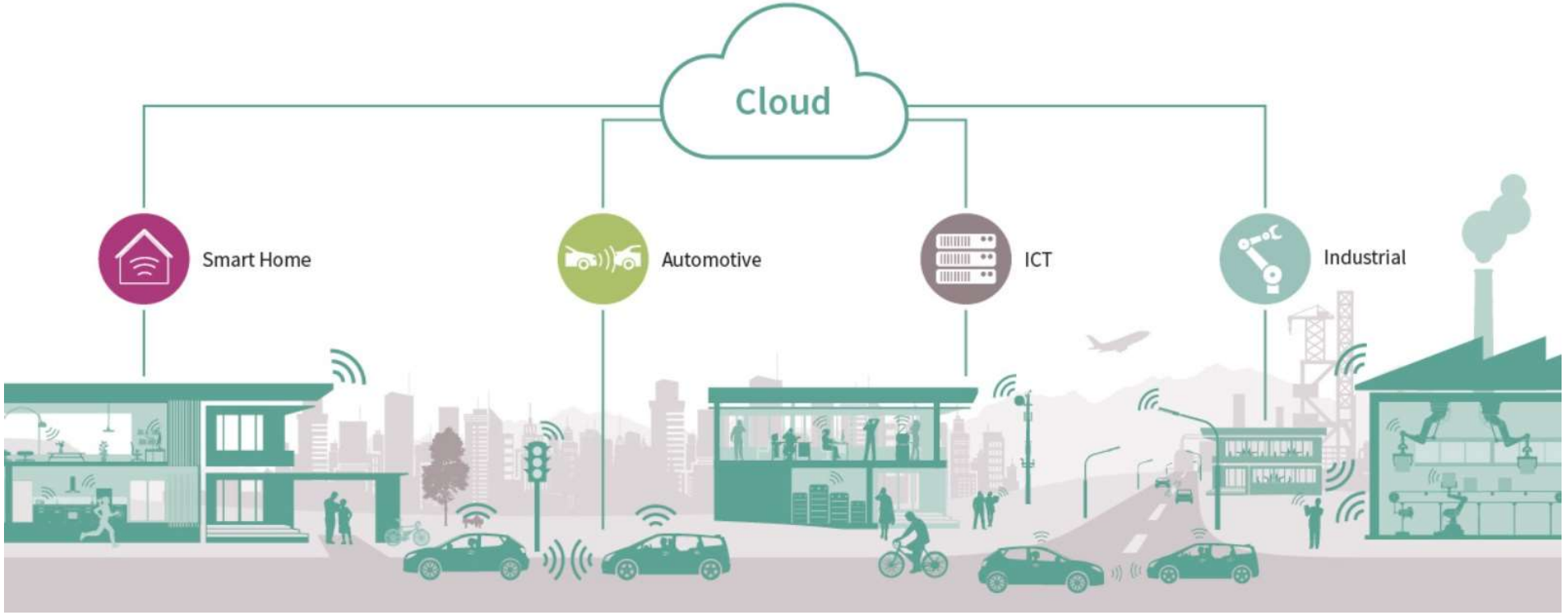


Table of contents

Focus of presentation: Security of CPS build on top of microcontrollers (MCUs)



- Security aspects for microcontrollers (MCUs) targeting smart home, automotive, ICT, and industrial
- Perspective from silicon vendor (i.e., Infineon) to (product) developer, to the end user

Major security challenges in CPS

Cyber Physical System (CPS) require specific care: If not protected, attackers may cause immediate physical harm to people (e.g. motor control)”

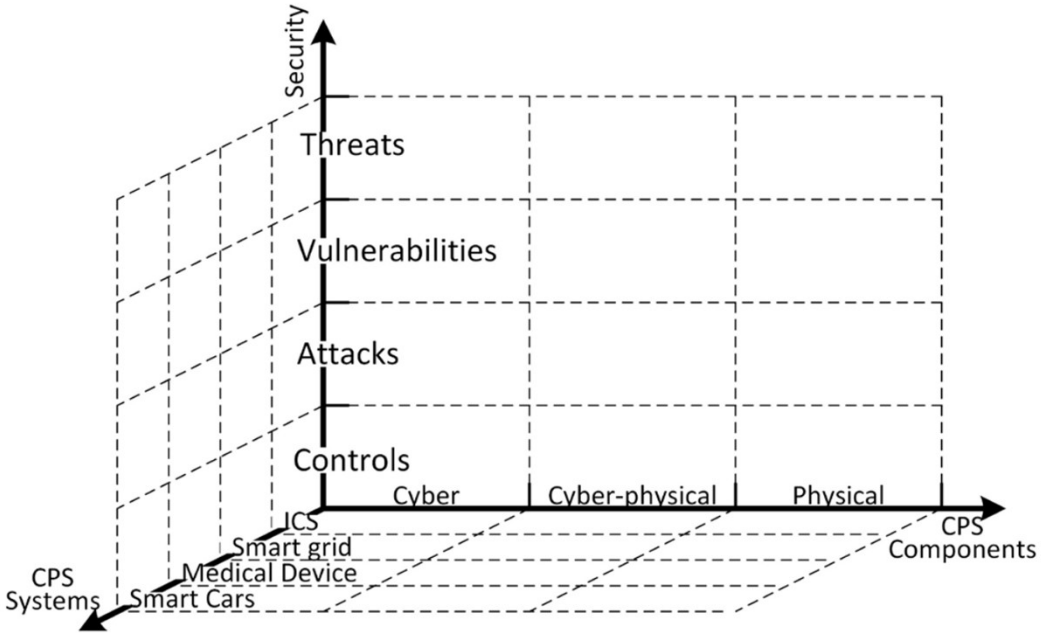
- Increasing degree of **connectivity** of CPS
  - Large scale attacks become possible over the Internet
  - Exploitation of device-2-device communication (e.g., Bluetooth)
- **Physical attack methods** and tools become more and more accessible and common (e.g., Chip Whisperer)
  - We need to consider “physical attack” in the threat model of CPS
  - Risks for IP extraction and analysis
- Increased **complexity and standardization** of SW stacks (e.g., RTOS)
  - Stacks become too complex for code review and need constant patching
  - Exploitation of security vulnerabilities during SW update

Systematic model for the security of CPS (Humayed at al., 2017)

- **CPS definition and key points**
  - Sensor and actuator networks are embedded
  - Heterogeneity of building blocks
  - Sensors, actuators, and embedded systems

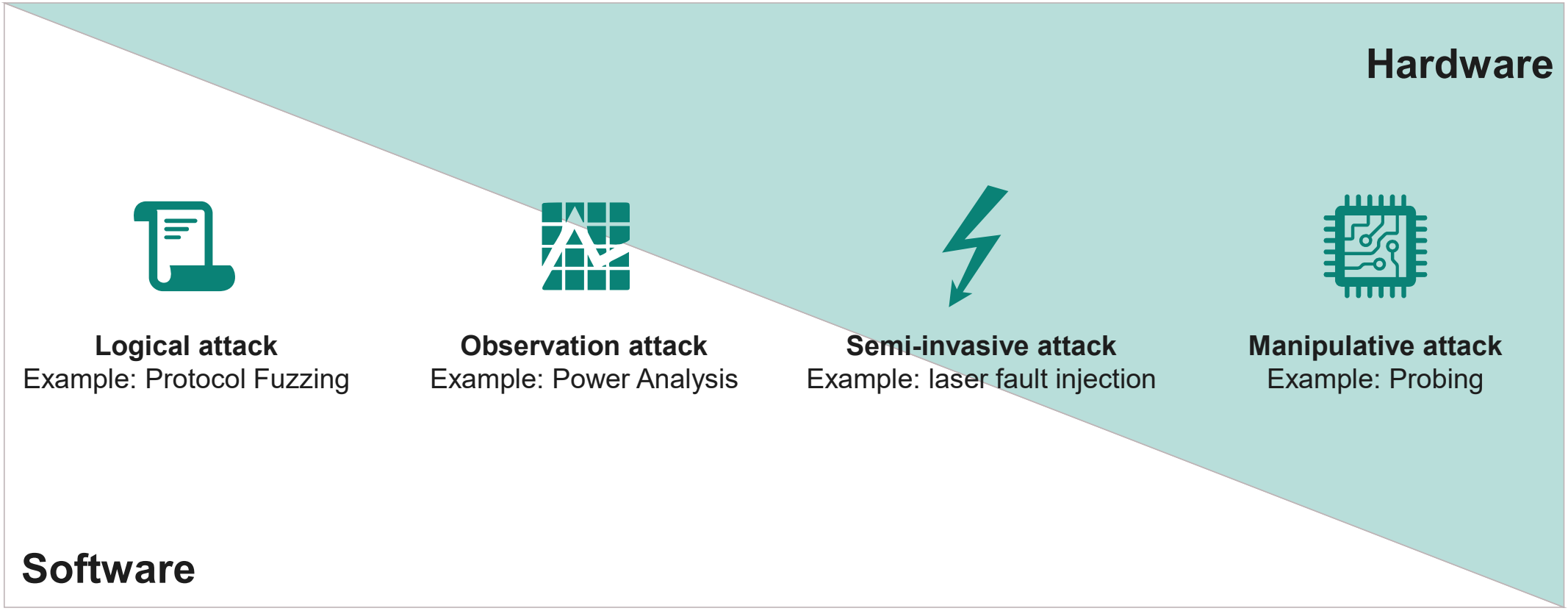
- CPS **general security challenges**
  - Security by Design: Security is often not considered
  - Cyber-Physical Security: Cyber-only security is not sufficient
  - Real-Timeliness Nature: Constraints on performance (e.g., crypto)
  - Uncoordinated Change: multiple stakeholder in heterogenous environment

- What happened since 2017 (**personal view**):
  - IoT goes cyber-physical: Lawnmowers, ovens, robot vacuum cleaner, door locks, climate control …
  - Stronger focus on resilience and recovery (NIST SP 800-160)
  - Emerging security regulations (e.g., EU Cyber Resilience Act)



Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security - A survey. *IEEE Internet of Things Journal*. https://ittc.ku.edu/~fli/papers/2017_iot.pdf

Attackers perform physical attacks on CPS devices to gain knowledge for developing a remote attack



Software (alone) cannot protect IoT devices sufficiently against attacks

Why is protection against physical attacks important? They are often used to discover new attacks

Attacker gets **physical access** to device

Often done: buying a "copy" of the targeted IoT device on the Internet

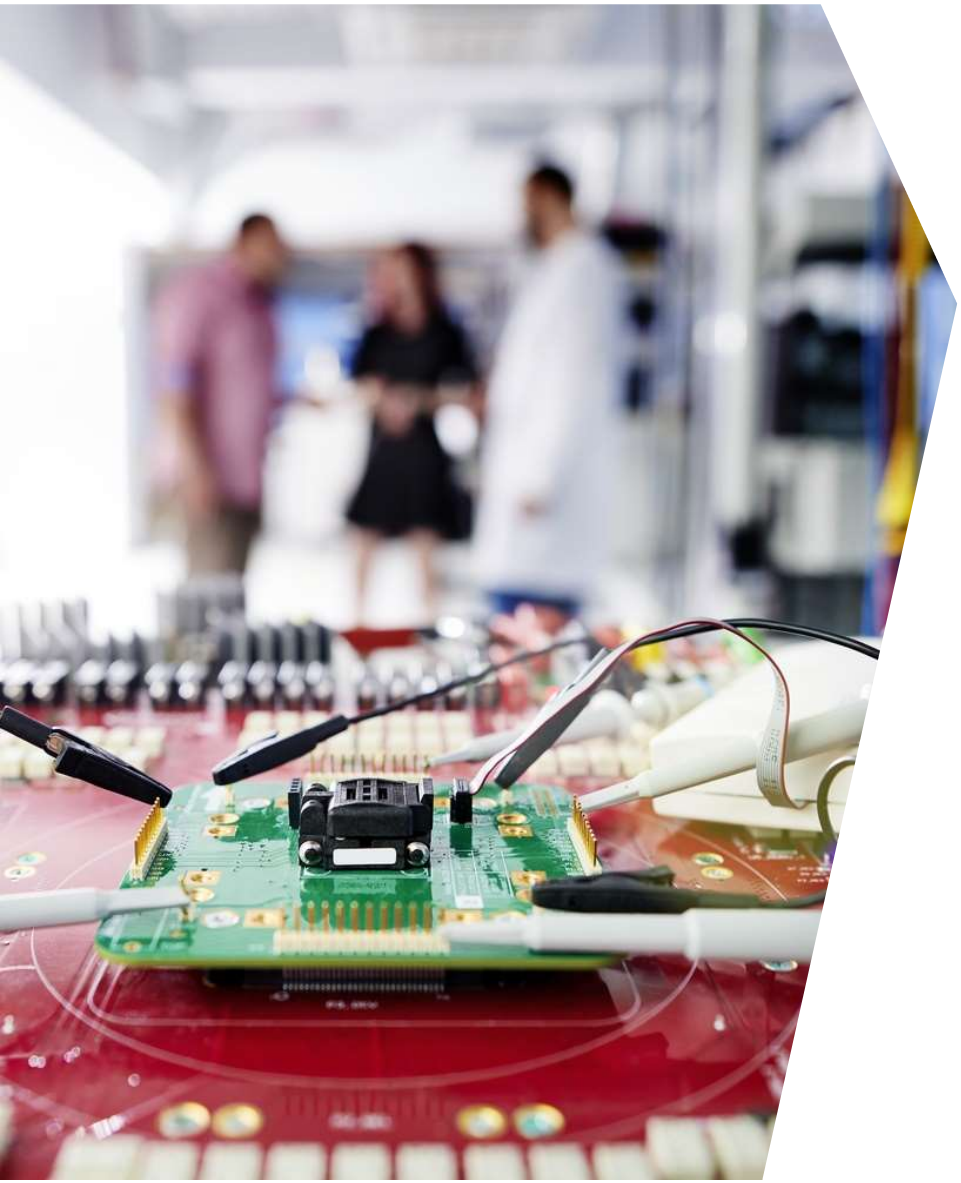
Attacker performs physical attacks to identify vulnerabilities

Examples of physical attacks

- Unsolder & read out flash memory to analyze SW
- Tampering of µC to identify sensitive information or cause unintended behavior

Attacker implements and performs remote attack

The attacker combines the know-how gained from physical attacks with other attack vectors to create a new attack



Example of physical attack

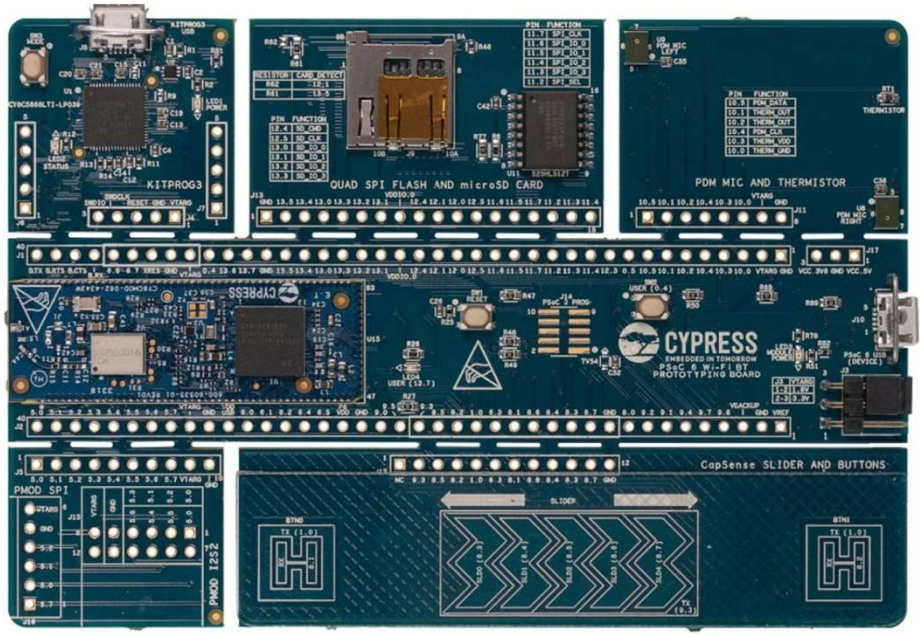
Fill your Boots: Enhanced Embedded Bootloader Exploits via Fault Injection and Binary Analysis

Jan Van den Herrewegen[1], David Oswald[1], Flavio D. Garcia[1] and Qais Temeiza[2]

[1] School of Computer Science, University of Birmingham, UK, {jxv572,d.f.oswald,f.garcia}@cs.bham.ac.uk
[2] Independent Researcher, qaiskhaled744@gmail.com

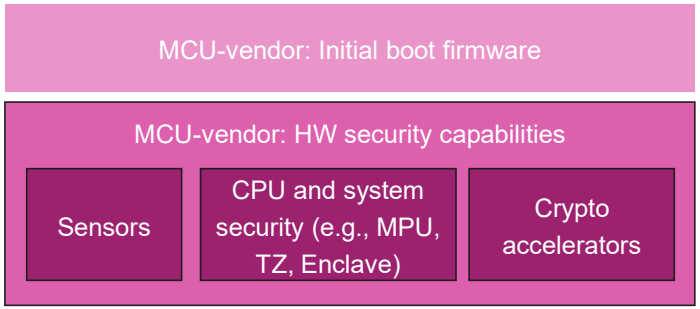
- Binary analysis and software exploitation techniques combined with voltage glitching
  - Return-Oriented Programming to exploit the bootloader of a microcontrollers
  - Dynamic analysis of a bootloader to constrain the glitch parameter search
  - Shows how to aim voltage glitches at target instructions

Table of contents



Lets see how a standard MCU works and how it contributed to CPS security

A typical MCU used in CPS (e.g., industrial control)

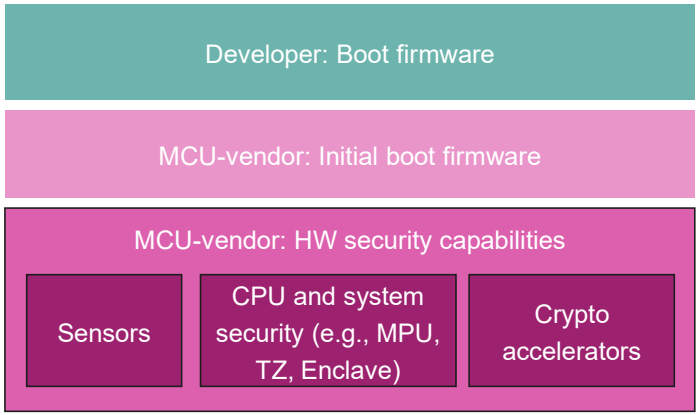


MCU- Vendor
HW security capabilities and boot firmware

- At tapeout the vendor defines a certain set of security functionality for an MCU (with future-proofing in mind)
  - Availability of crypto accelerators
  - Availability of security functions (e.g., system Memory Protection Unit, Trust Zone)
  - Sensors to detect abnormal operating conditions (e.g., temperature)

- The MCU vendor defines a boot firmware (in ROM and/or NVM) that configures the MCU and its security functionality
  - Secured boot
  - Debug protection
  - Lifecycle state management

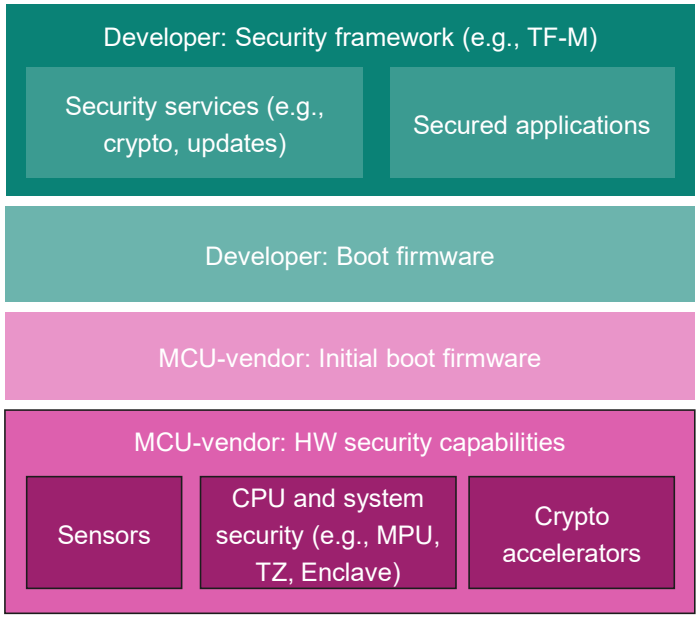
A typical MCU used in CPS (e.g., industrial control)



Developer Boot firmware

- Developer defines code executed after MCU boot is finished
  - Additional setup of hardware
  - Update capabilities (e.g., over a serial interface)
  - Disabling or enabling of debugging options

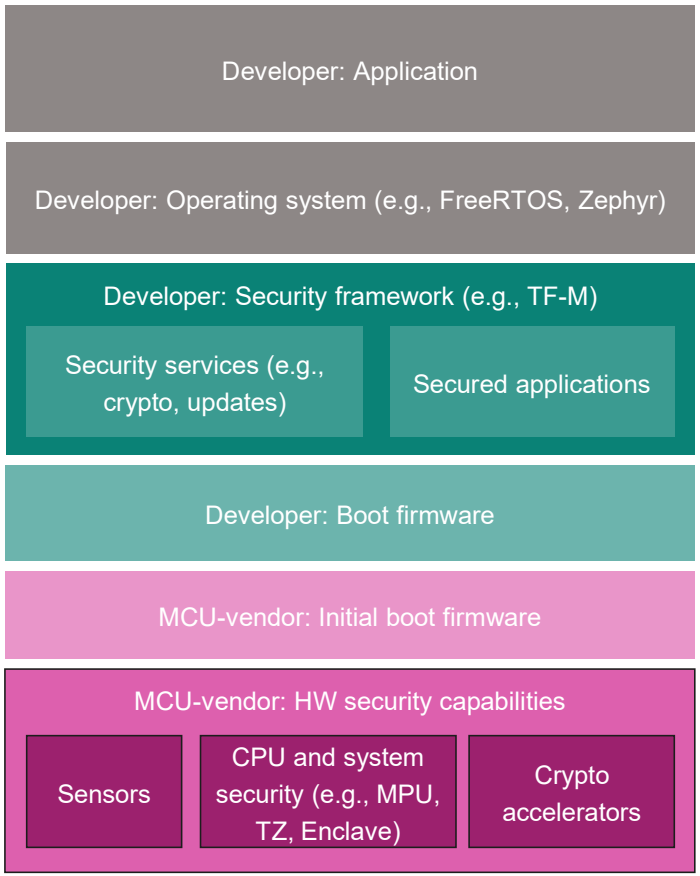
A typical MCU used in CPS (e.g., industrial control)



Developer
Security framework (e.g., TF-M)

- Most prominent security framework today is Trusted Firmware-M (TF-M)
  - Secure Processing Environment (SPE) for Armv8-M, Armv8.1-M architectures
  - Enables certification according to platform security architecture (PSA)
  - Controls the isolation, communication, and execution of Secure (S) and Non-Secure (NS) code
- Functionality
  - Secured Boot for firmware authentication
  - Crypto, Internal Trusted Storage (ITS), Protected Storage (PS), Firmware Update and Attestation security services
  - Secured Applications: Application Root of Trust services

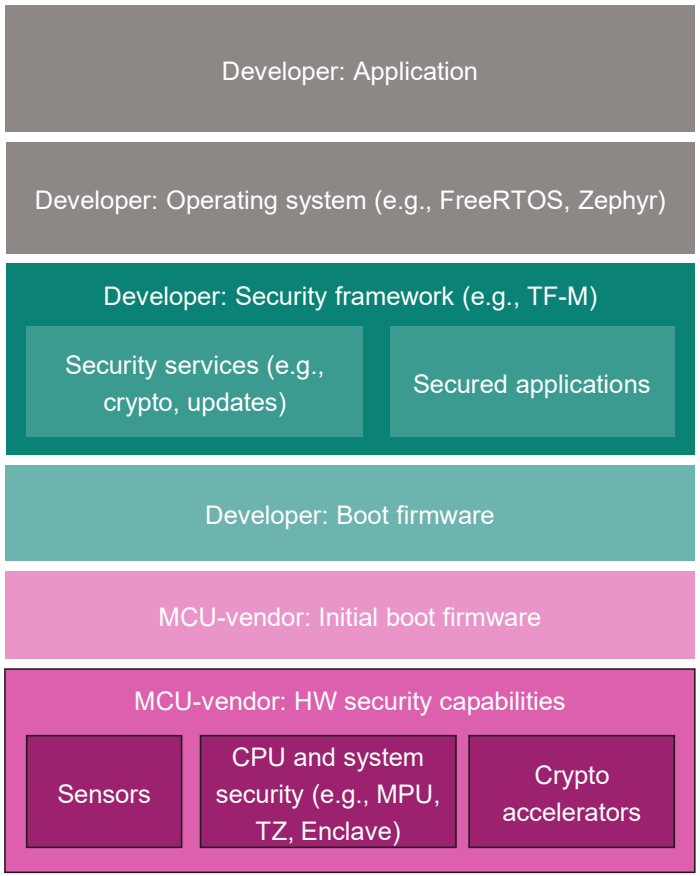
A typical MCU used in CPS (e.g., industrial control)



Developer
Application and Operating system

- Operating system (optional)
  - Kernel and supporting services (Linux is often too big)
  - Hardware abstraction
  - Protocols (e.g., TCP-IP) and connectivity services (e.g., Bluetooth, Wifi, USB)
  - Cloud integration
  - Over-the-air updates
- Application
  - Implements logic of the CPS
  - Gathers sensor data
  - Control actuators
  - Connects to other devices and the cloud

A typical MCU used in CPS (e.g., industrial control)



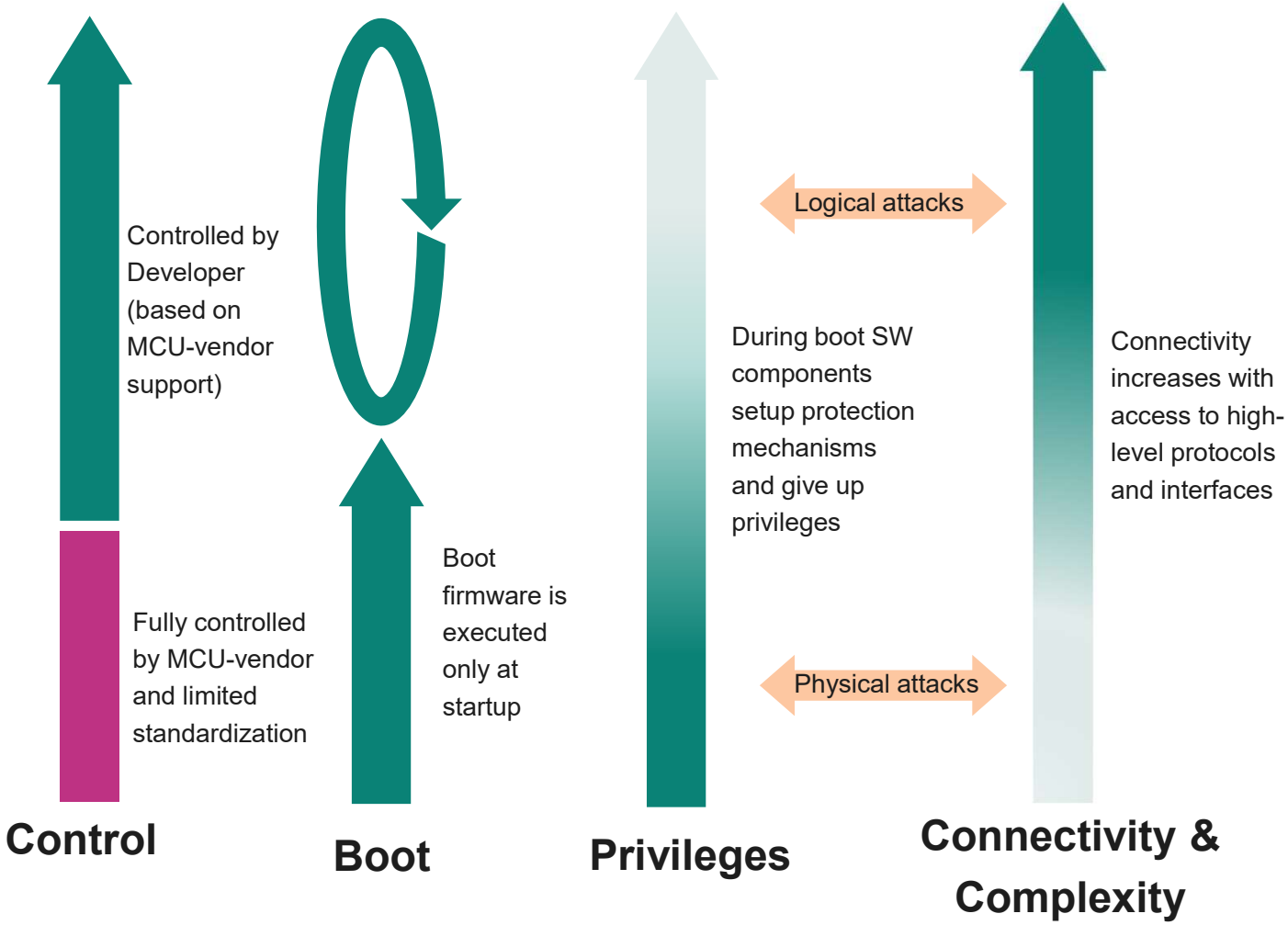


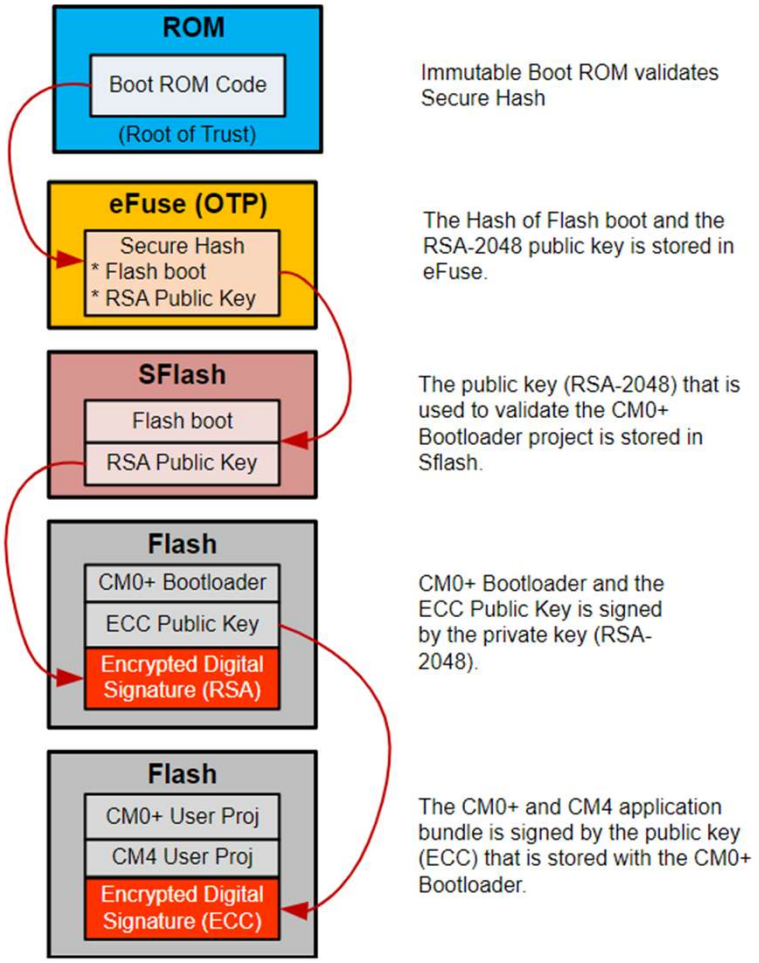
Table of contents

Challenge: Firmware verification vs. Boot time

- Secured Boot (also Trusted or Measured Boot)
  - Device starts out of a protected root-of-trust (RoT) like ROM
    - RoT verifies authenticity of next firmware component prior to execution
    - Hashing and comparison against value in OTP (immutable) or verification of firmware
  - Repeated for each subsequent component

- Challenges
  - Limited availability of eFuses to implement OTP in newer process nodes
  - Multi-stage boot requires verification of multiple firmware components
  - Large NVMs need time for verification – contradicting real-time requirements

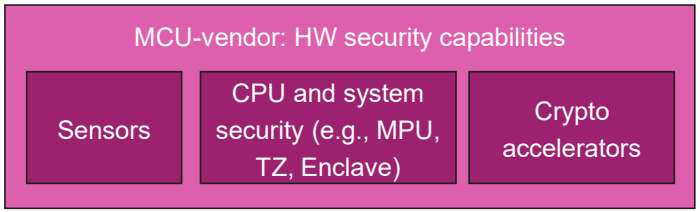
- Research challenge
  - Secured Boot concepts for firmware verification that enable reasonable boot time



PSoC64 Secured Boot process
https://documentation.infineon.com/html/psoc6/isi1667483210870.html

Challenge: Crypto agility and support

- CPS need to support state-of-the-art cryptographic schemes
  - Key exchange
  - Signature schemes
  - Symmetric schemes
- MCU-vendors decisions are crucial
  - Selection of crypto accelerators
  - Selection of CPU for SW implementation



- Challenge
  - MCU-vendor: Correct product positioning in terms of price and features
  - Developer: Availability of all required cryptographic accelerators (at the correct security level)
  - Development of cryptographic software according to standards (e.g., ASPICE)
- Research challenge
  - Flexible accelerators
  - Implementations that support a wide range of schemes

Quantum Computers and their consequences to CPS

Large-scale QC threatens public-key cryptography

- Shor's quantum algorithm will eventually break currently used public-key cryptography (RSA & ECC)
- … thus endangering services like Digital Signatures, Secret Key Exchange, PKI …

We don't know when RSA/ECC will be broken, but…

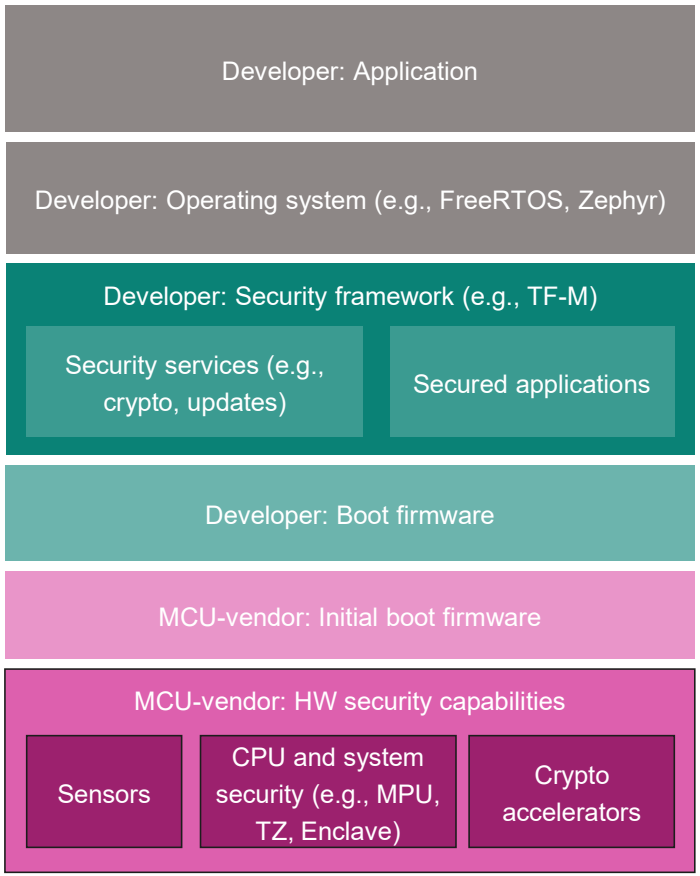
- leadup time to deploy new solutions
- time in production
- long lifetime of components in the field
- long-term secrecy (store-now-decrypt-later)
- cryptographic transitions notoriously slow in the past

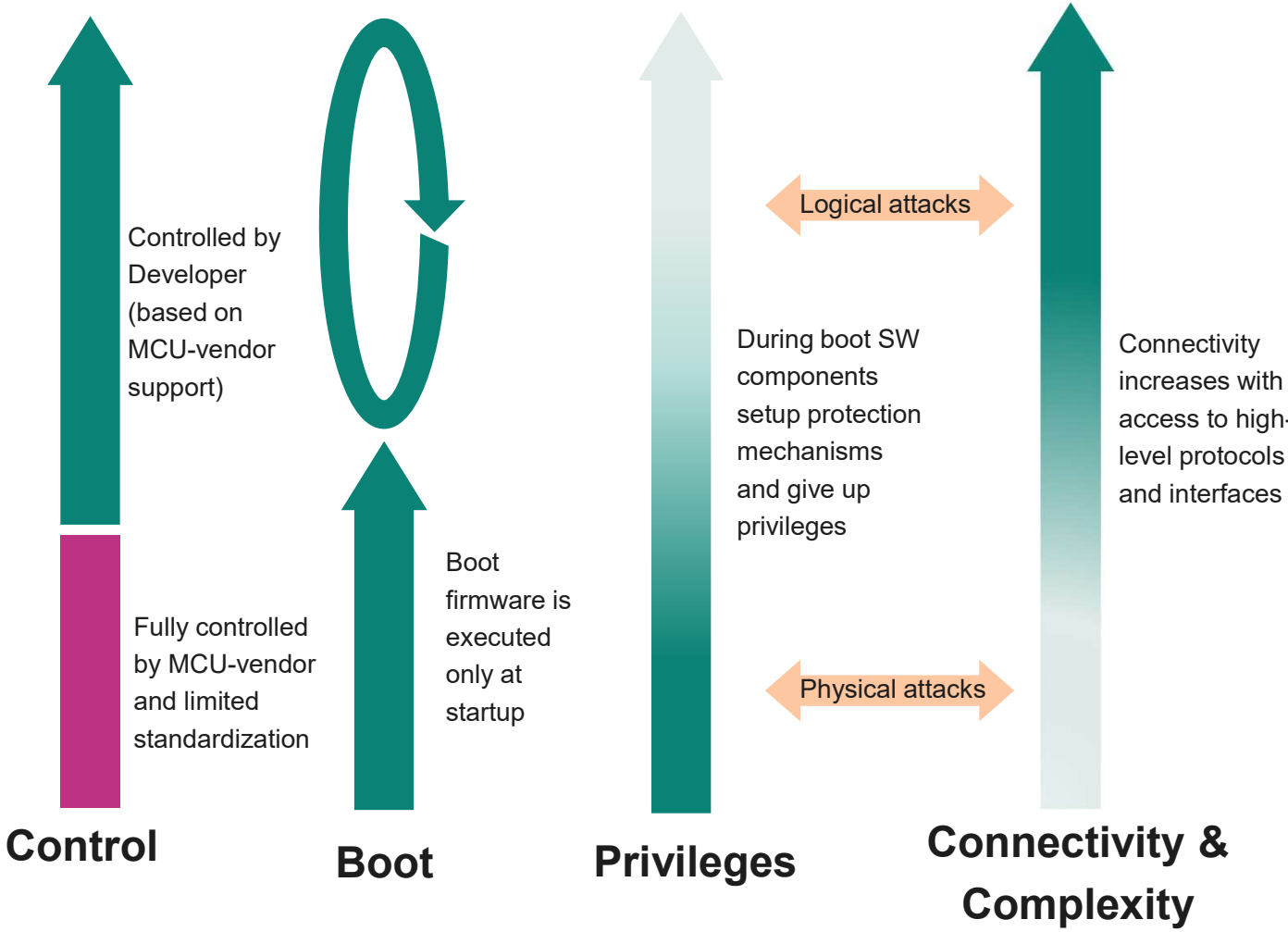
NIST standardization process

Selected algorithms (NIST primary options)
Key encapsulation: Kyber, FIPS203 "**ML-KEM**"
Signatures: Dilithium, FIPS204 "**ML-DSA**"
Stateful Signatures ("fast track"): **XMSS & LMS**, NIST SP800-208

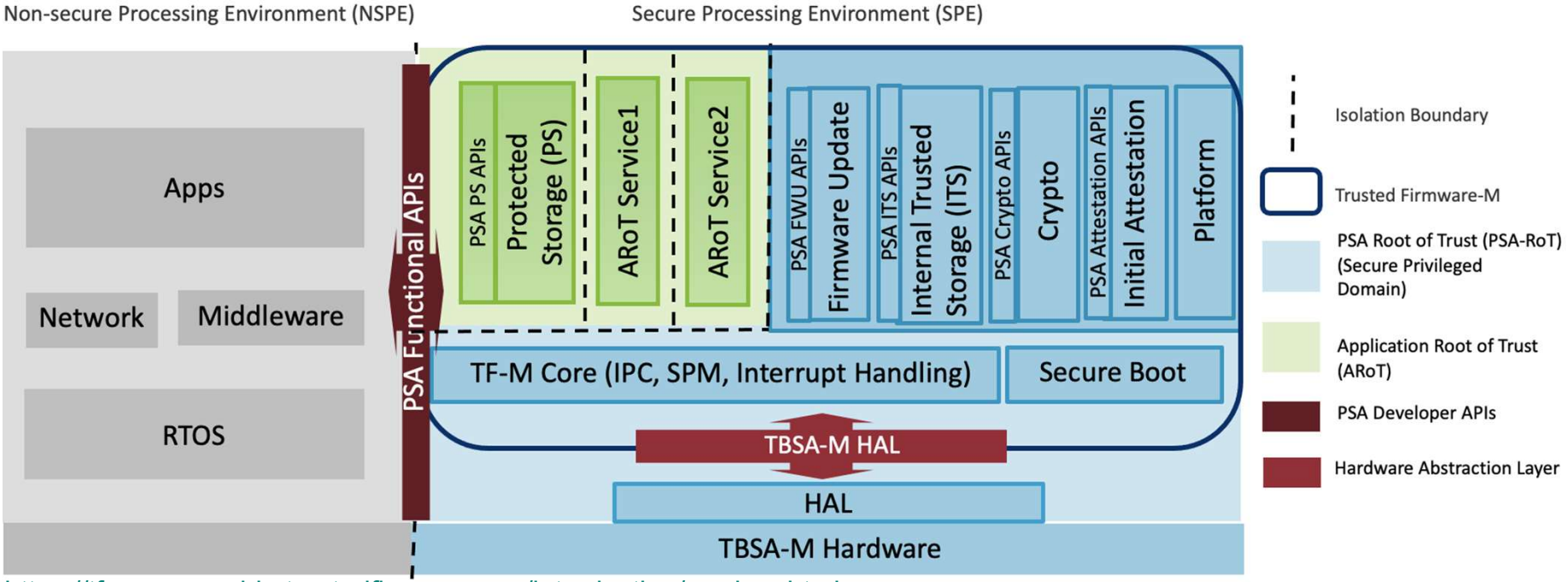
Runtime: more complex HW acceleration
ML-KEM / ML-DSA: many different subcomponents
XMSS / LMS: hashing (SHA2 / SHA3

A typical MCU used in CPS (e.g., industrial control)





TFM-M is a complex security framework



https://tf-m-user-guide.trustedfirmware.org/introduction/readme.html

- **Partitioning of CPS**
- Security analysis
- **Use-cases**
- Cost vs. benefit
- Physical protection
- Maintenance

Multiple voltage faults are practical

Oops..! I Glitched It Again! How to Multi-Glitch the Glitching-Protections on ARM TrustZone-M

Xhani Marvin Saß, Richard Mitev, and Ahmad-Reza Sadeghi,
Technical University of Darmstadt

https://www.usenix.org/conference/usenixsecurity23/presentation/sass

- Voltage glitching to inject multiple coordinated faults
- Novel flow for Multiple Voltage Fault Injection (MVFI)
- Able to overcome some fault countermeasures

Table of contents

External requirements for stronger security

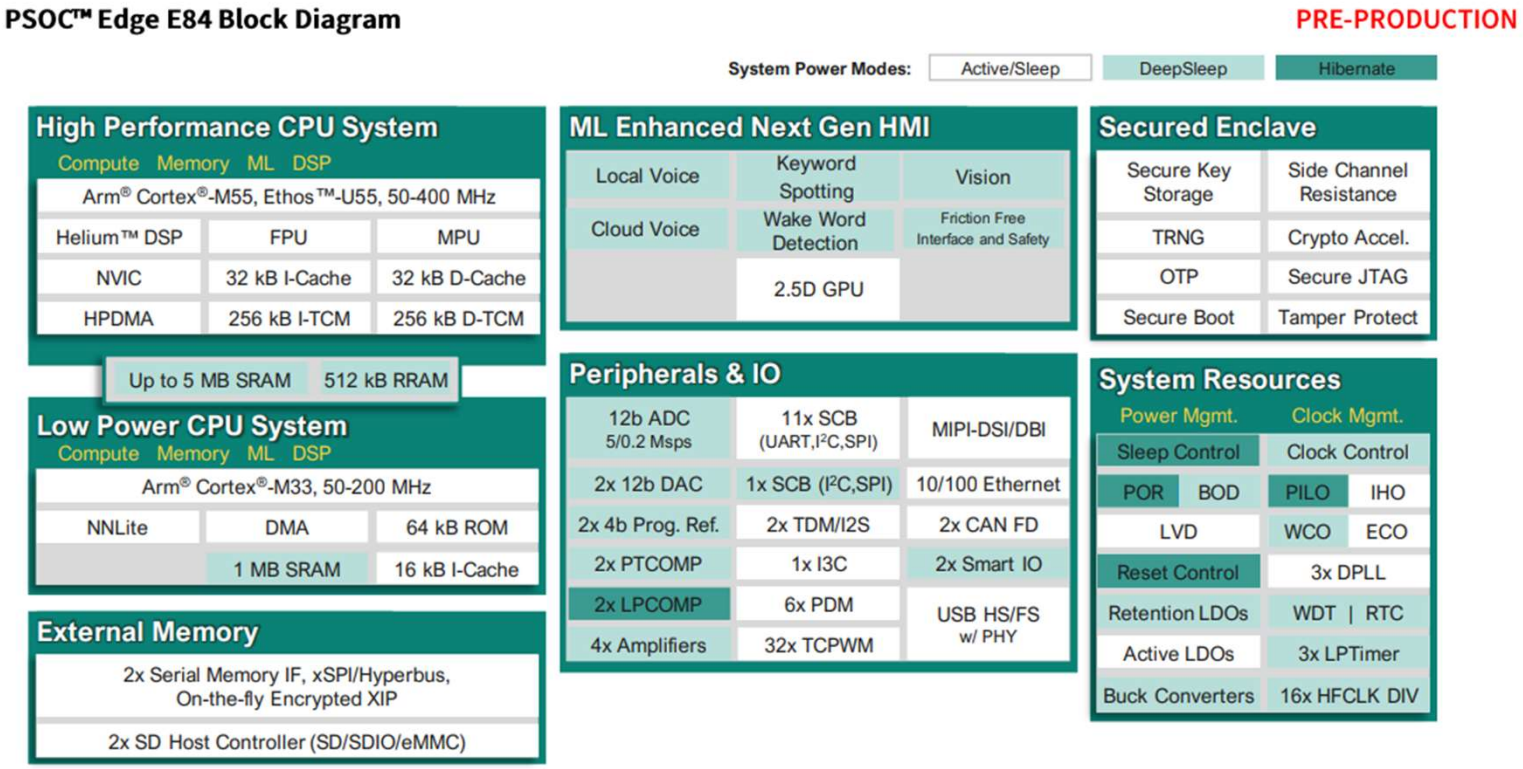
- Standards and regulations
  - NIST IR 8425 (Profile of the IoT Core Baseline for Consumer IoT Products
  - European Union (EU) EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements)
  - Singapore Cybersecurity Labeling Scheme (CLS)
- Certification schemes
  - Security Evaluation Standard for IoT Platforms (SESIP)
  - Platform Security Architecture (PSA)
- Personal option
  - May not be very visible from academic perspective
  - Some requirements sound trivial
  - Will have long term impact on the industry

Generic requirements from standards

1. Unique identity for each IoT Device
2. No hardcoded default passwords
3. Secured storage of sensitive data on the Device
4. Secured communications of security-relevant information
5. Secured software updates throughout the support period
6. Secured development process, including vulnerability management
7. Public documentation regarding security, including the support period

https://community.infineon.com/t5/Blogs/Infineon-Leads-in-IoT-Security-Certification/ba-p/716276

PSOC™ Edge E84



State-of-the-art Security

- Lockstep secured enclave in low-power always-on domain
- Infineon Edge Protect Category 4
- Off-the-shelf Trusted Firmware-M enablement and Mbed-TLS for crypto operations

See https://www.infineon.com/dgdl/Infineon-PSOC_Edge_E84-ProductBrief-v01_00-EN.pdf?fileId=8ac78c8c8d2fe47b018e7a274d657378

Infineon is hiring a PhD student in SW security

Scope of the PhD thesis in cooperation with TU Munich

- **main areas** of research activities are **AI** and **fuzzing**
- **main topics** for the PhD work
  - reduce manual effort for fuzzing (e.g., automatic harness creation, automatic rehosting) with AI support
  - improve quality of fuzzing campaigns (e.g., Good-Turing-Criteria) by AI guidance
  - detection of unsecure or weak code with AI
  - assessment and development of a proof of concept for AI-supported software attacks

Interested?

Please contact Wolfgang.Rankl@infineon.com

as soon as possible or talk to me

https://www.infineon.com/cms/en/careers/jobsearch/jobsearch/HRC0760522-Doctoral-Thesis-AI-Technologies-for-Security-f-m-div/

Conclusion

- Security in CPS is challenging due to the inherent complexity of CPS itself
- The industry is moving fast and heavily impacted by new regulations (e.g., CRA) and certifications (e.g., PSA)
- Interesting security research opportunities for HW, HW/SW and SW

Thank you for your attention!

Any questions?

Contact

http://tpoeppelmann.de

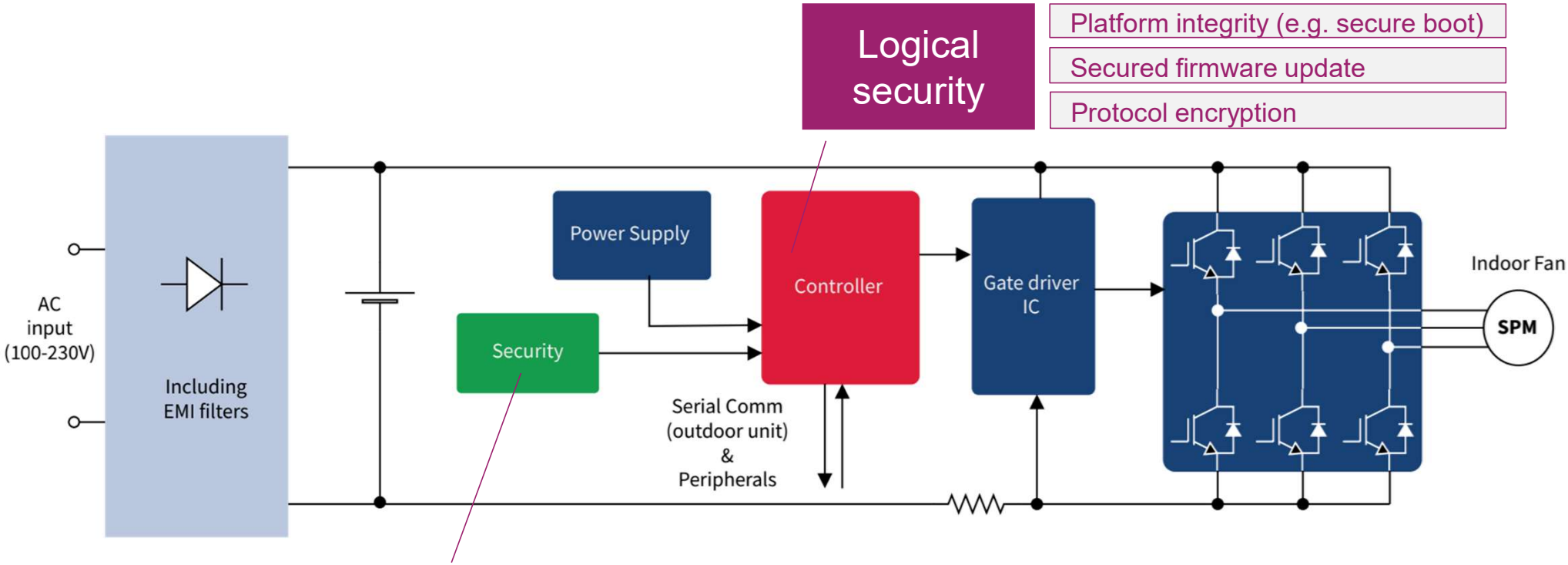
Thomas.Poeppelmann@infineon.com

Infineon is hiring:

https://www.infineon.com/jobs


infineon

Case study: Residential aircon




infineon