VRIJE UNIVERSITEIT BRUSSEL

TrustedIoT

Introduction to Embedded Security
June 9th 2023

Laurent Segers
An Braeken
Abdellah Touhafi
Bruno da Silva

AGENDA

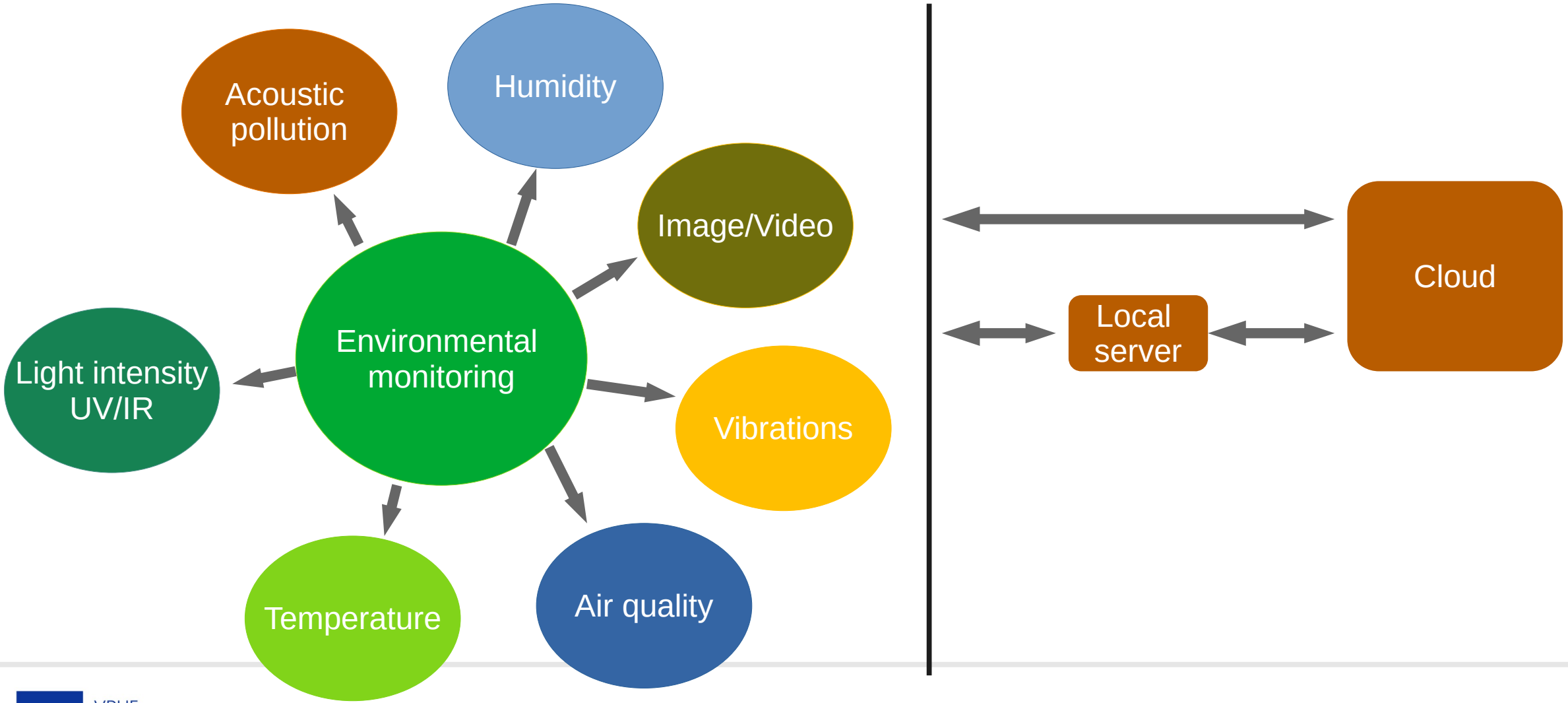
- Target applications – environmental monitoring
  → Low-throughput vs. High-throughput sensing

- Security risks and mitigation

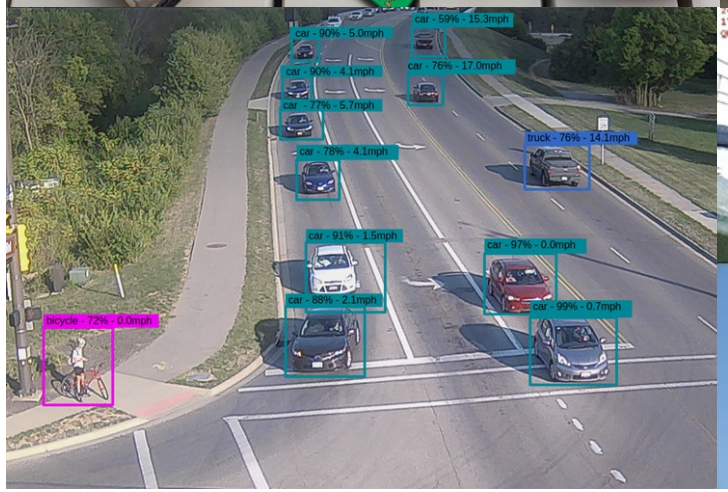
- Low-throughput sensing platforms
  → low-end platforms
  → security features
  → selection
  → implementation
  → goals and next steps

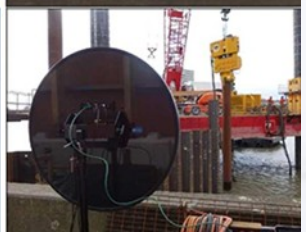
- High-throughput sensing solutions
  → mid- and high-end platforms
  → next steps

VUB USE CASES – ENVIRONMENTAL MONITORING

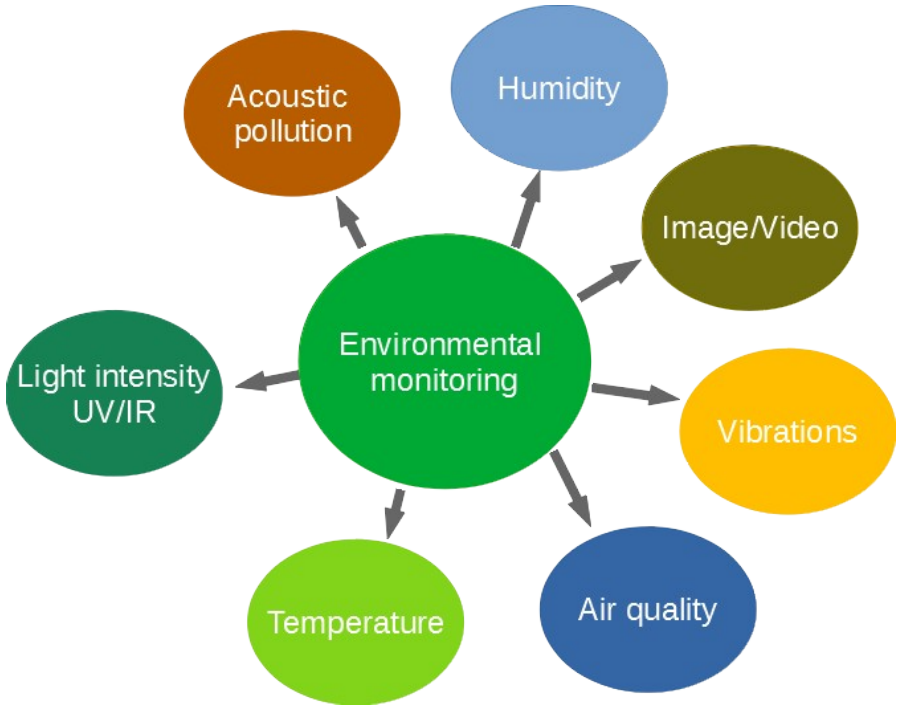


VUB USE CASES – ENVIRONMENTAL MONITORING





VUB USE CASES – ENVIRONMENTAL MONITORING



Local temperature and humidity
→ impact of arrangement

Vibration
→ impact of traffic, excavations, crowd movement

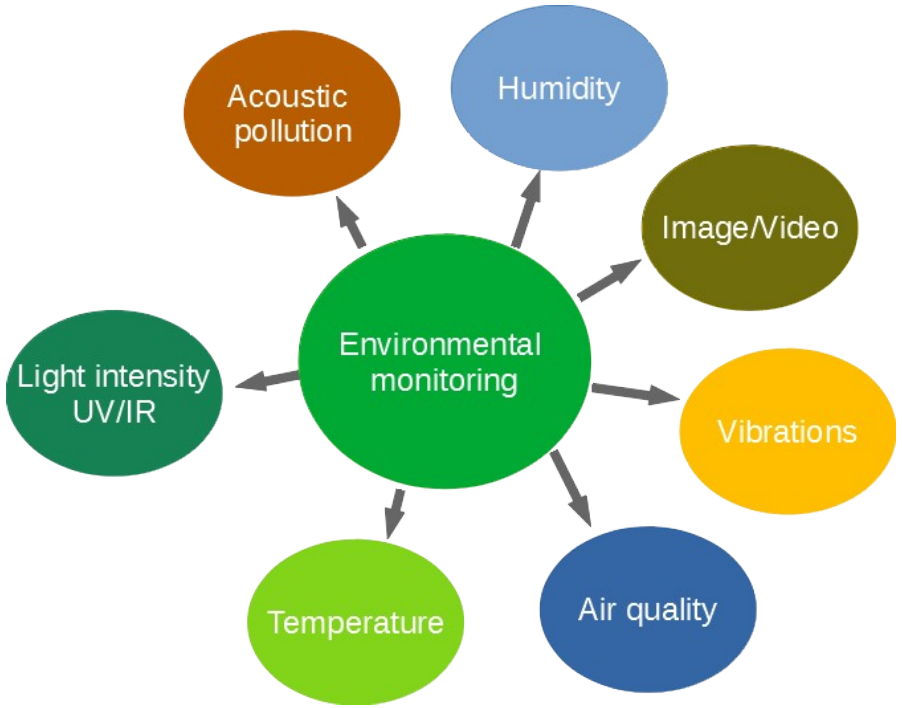
Acoustics (quiet, loud)
→ Sound pressure level (SPL), type of sound, etc.

Air quality
→ Particle detection, pollution induced by traffic

CO2
→ Locally emitted by traffic, older households, etc.

Light, UV, IR
→ Light pollution, irradiance detection

VUB USE CASES – ENVIRONMENTAL MONITORING



Low-throughput sensing

- Sound pressure level
- Temperature / humidity
- Vibration events
- Air quality / light

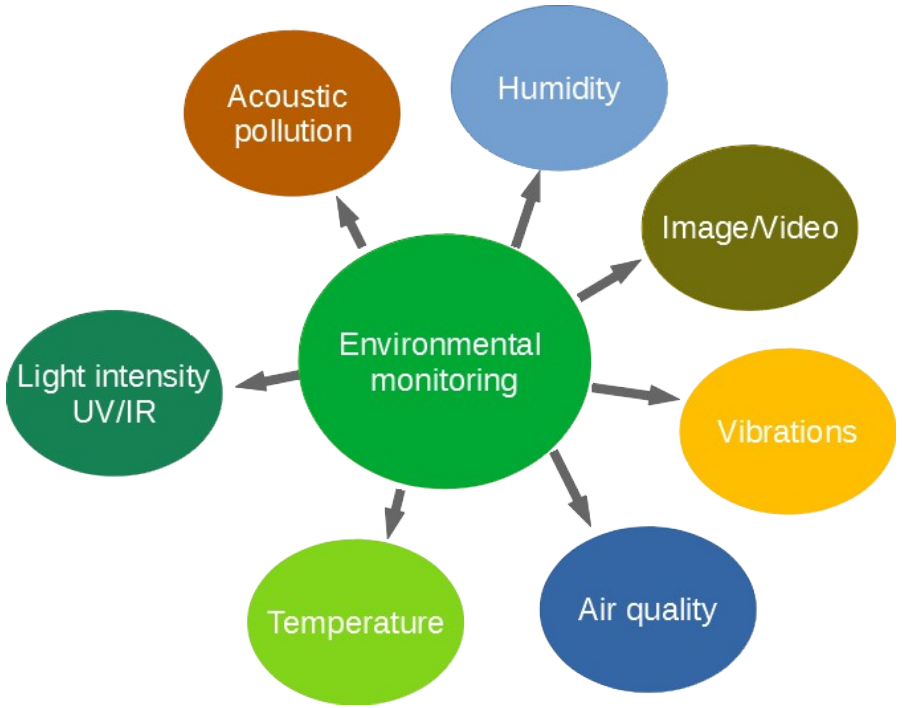
High-throughput sensing

- Audio and/or video (array of sensors)
- Fine-grained analysis

Risk for data authenticity / leakage / GDPR → security?

VUB USE CASES

LOW-THROUGHPUT SENSING RISKS

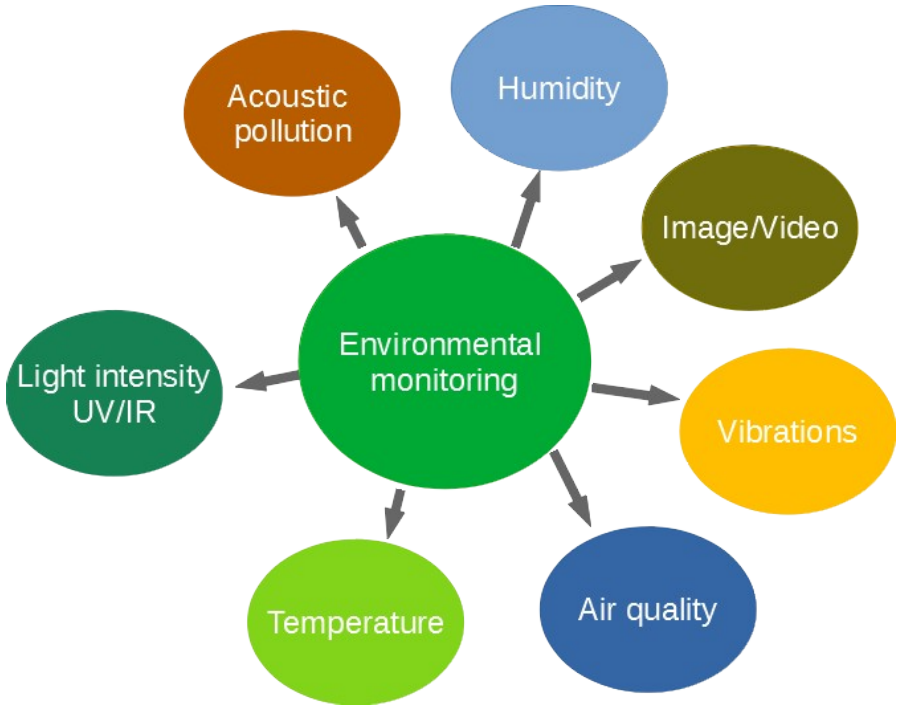


Risks & mitigation

- Moving device to other location
  Location awareness (GPS) can mitigate security risks
- Wireless communication → spoofing, jamming, read-out of data, data alternation
  → *Store jammed data locally until successful retransmission*
  → *Encryption/integrity protection of transmitted data*
- Modifying/Reading of locally stored data
  Data encryption, data integrity check
- Firmware (mis)configuration
  → *integrity test during attestation*
- Over the air updates compromised with spoofed firmware/configuration
  → *Authentication + encryption of firmware*

VUB USE CASES

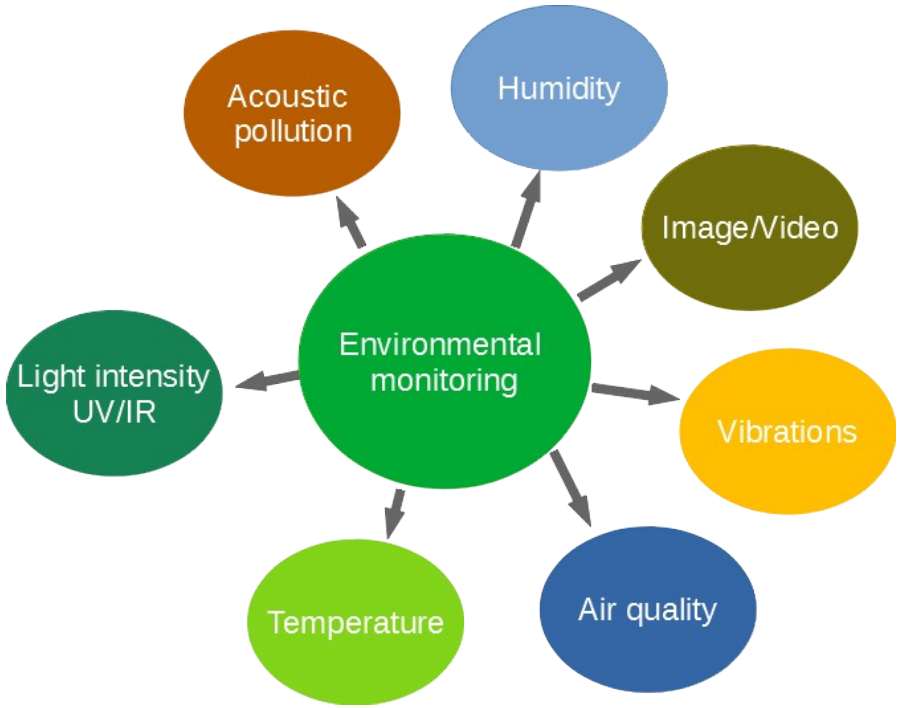
HIGH-THROUGHPUT SENSING RISKS



Risks & mitigation

- Comprises minimally same set of risks as low-end devices + in addition:
  - Firmware (mis)configuration
    → *integrity test during attestation*
  - Over the air updates compromised with spoofed firmware/configuration
    → *Authentication + encryption of firmware*
- Unauthorized access by third party
  → all communications are authenticated and encrypted
- Read-out/manipulation of audio/video streams!
  → encrypt data locally before transmission/storage

VUB USE CASES



Low-throughput sensing

- Low-end devices (e.g. IoT devices)
- Limited resources (processing, memory,…)
- Limited security (if any)
- But still… security is needed!

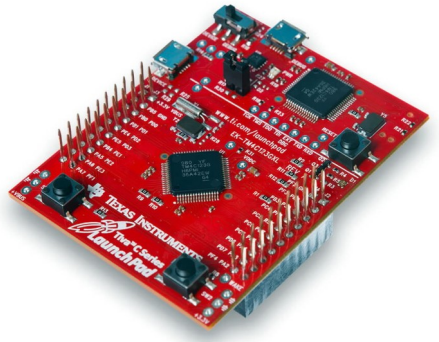
High-throughput sensing

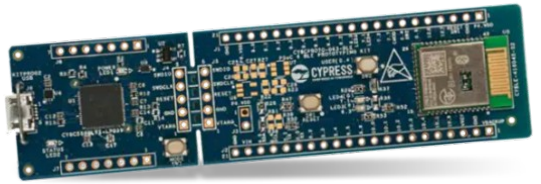
- Mid- and high-end embedded platforms
- Single and multi-core computing
- SoC, TPU, MPSoC, etc.
- More advanced security are required

VUB USE CASES

LOW-END PLATFORMS SECURITY REQUIREMENTS

- Minimal Hardware-based isolation if possible
  → TrustZone
- Basic Root-of-Trust (for some applications)
- Secure boot
- Secure bootloaders
- Trusted peripherals (when possible)
- Optimizations for secure storage
- Secure over the air updates
- Low-power





LOW END DEVICES AND PLATFORMS

NXP/FREESCALE SECURE PLATFORMS

Few families with security features:

- Many MCUs equipped with Memory Protection Unit (MPU)

- LPC5500-series based on the ARM-Cortex-M33 MCUs.
  → TrustZone
  → SRAM PUF-based RoT
  → Real-time code execution from encrypted images (internal flash)

- C29x (C291-C293) Crypto Coprocessors
  → Up to 32k RSA 2048-bit private key
  → Accelerated AES-HMAC-SHA-1 bulk encryption
  → Public key and secure key management
  → Secure boot, tamper detection, optional battery backed secret key
  → NIST compliant random number generator

LOW END DEVICES AND PLATFORMS

STM SECURE PLATFORMS

STMicroelectronics offers a few families with security features:

- ST23 for financial transactions: banking, e-government solutions, smart-card for pay-TV, etc.
- STM32 based on ARM-Cortex-M33 (STM32L5 and STM32U5) ultra-low-power MCUs.
  → relies on TrustZone
- ST33 series implement TPM 2.0 modules used in personal computers, servers and automotive industry
  → on I2C and/or SPI interface

LOW END DEVICES AND PLATFORMS

MICROCHIP MICROCONTROLLERS

PIC32CM LS60/LS00 based on the ARM-Cortex M23 MCU
→ TrustZone
→ Secure subsystem via ECC608 Trust Platform
→ Cryptographic modules integrated

SAM E5x based on the ARM-Cortex-M4F
→ Tightly coupled memory architecture, MPU
→ Symmetric/Asymmetric encryption

CEC173x Trust Shield (ARM-Cortex-M4F) real-time RoT controllers for servers, telecom and networking

LOW END DEVICES AND PLATFORMS

NXP/Freescale	STMicroelectronics	Microchip
LPC5500-series based on the **ARM-Cortex-M33 MCUs**	STM32 based on **ARM-Cortex-M33** (STM32L5 and STM32U5) ultra-low-power MCUs	PIC32CM LS60/LS00 based on **ARM-Cortex M23**
• TrustZone • Energy efficiency • SRAM PUF-based RoT • Encrypted images • ~ 4.5€/pc (1000pc)	• TrustZone • Ultra low-power • Cryptographic modules integrated • ~7.5€/pc (1000pc)	• TrustZone • Ultra low-power • Cryptographic modules integrated • Exist in secure and non-secure variants • ~4€/pc (1000pc)

LOW END DEVICES AND PLATFORMS

COMMON DENOMINATOR - ARM TRUSTZONE

TrustZone (Trusted Execution Environment): adds concept of Secure Monitor on top of user, kernel and/or hypervisor code. Deployed using RoT, CoT, safe boot and/or safe bootloader.

Advantages:

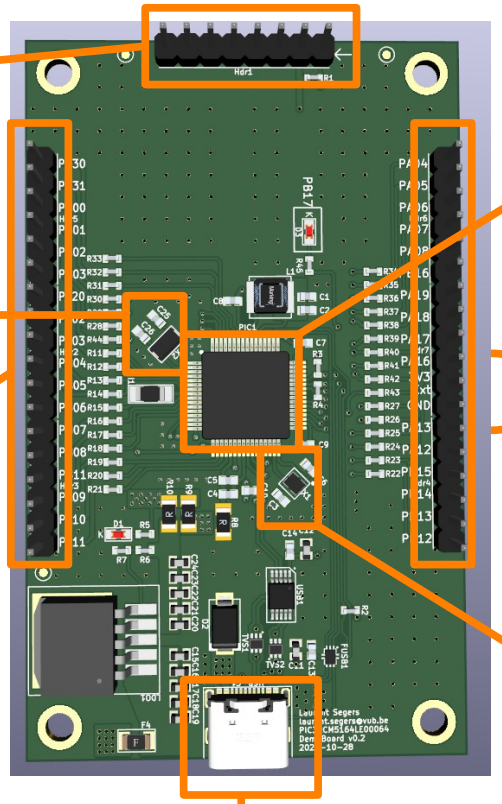
- More efficient in hardware overall design effort compared to dedicated secure sub-systems
- Can be used on peripherals
- Still allows full power of the main cores
- Isolation of secure/non-secure code

However:

- Not the whole code can be moved to TEE → careful organization of the code
- IDE or programming environment must be able to handle TrustZone code

LOW END DEVICES AND PLATFORMS

PIC32CM5164 ARM23-BASED LOW-END EMBEDDED PLATFORM



Programming header

RTC @ 32kHz

IO (+interruptable IO)
Sercom (SPI, I2C, UART)

PIC32CM5164L**E**00064 (non-secure)

PIC32CM5164L**S**00064 (secure)

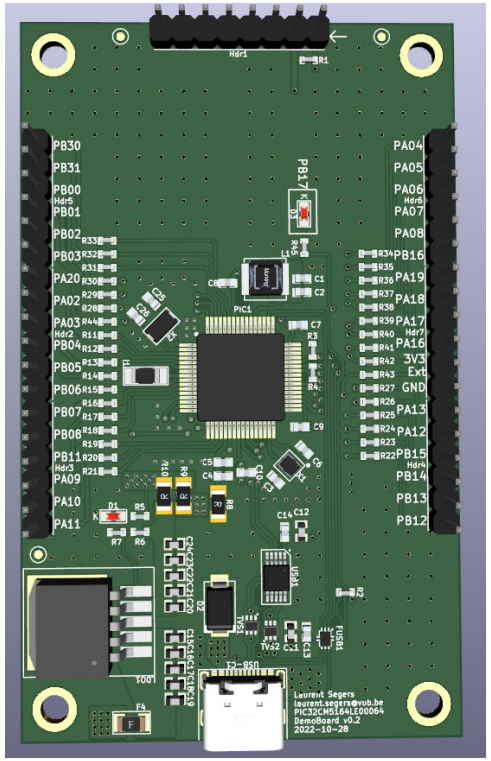
External power

Main crystal @ 32MHz

USB for power over USB + commucation to PC

LOW END DEVICES AND PLATFORMS

PIC32CM LOW-END EMBEDDED PLATFORM WITH TRUSTZONE



Based on ARM23 core platform with 512kB flash, 64kB SRAM, 32kB boot ROM

Offers TrustZone (5 regions in flash, 2 regions in data flash and 2 regions in SRAM)

1 TRNG, AES-256/192/1287, SHA-256

Public key validation support, 1 internal sign private key attestation

Secure boot with customizable secure boot public key

Optimized for secure storage + TrustRAM

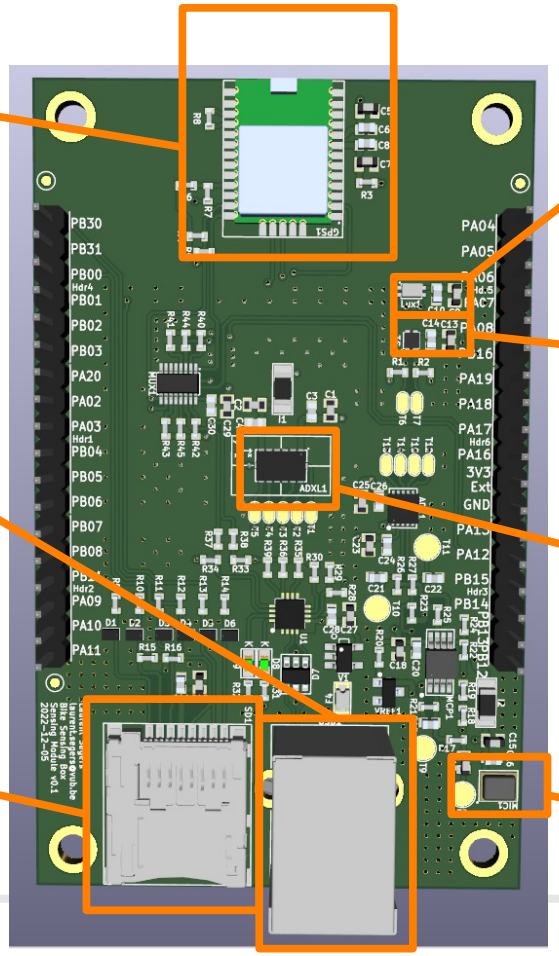
Up to 8 anti-tamper output IO + secure pin multiplexing to isolate secure communication channels

Unique 128-bit serial number

Separate registers for secure and non-secure application

LOW END DEVICES AND PLATFORMS

LOW-END SENSING MODULE



GPS (L96-M33)

VEML3328
light sensor (RGB+IR)

SHT41 temperature +
humidity sensor

UART to USB
communication to PC

ADXL343 3-axis
accelerometer

SD-card for logging

SPU0410LR5H-QB analog
microphone + SPI ADC

LOW END DEVICES AND PLATFORMS

PROGRAMMING ENVIRONMENT

IO, communication, memories, clocks, etc. can be configured with MPLab X IDE (6.x) + Harmony

Code generation of drivers and configuration → engineer focuses on applications

PIC32CM5164LE00064 is programmed as any other non secure micro-controller from MicroChip with only 1 application

PIC32CM5164LS00064 is programmed with 3 applications:

1) Secure bootloader: launches during boot and launches secure application first
2) Secure application with defined memory regions and secure registers
3) Non-secure code/application

LOW END DEVICES AND PLATFORMS

GOALS & NEXT STEPS

Evaluation of the power consumption differences between secure and non-secure platform

Measure time-impact of secure options compared to non-secure application

Optimize sensor module to also cover air-pollution and digital microphone (instead of analog)

Add wireless communication for remote data transmission

Remote programming of application

USE CASES

HIGH-THROUGHPUT SENSING PLATFORMS

Processing of audio and video

- Can be a single camera or microphone
- Array of microphones, multiple types of cameras
- Allow fine-grained monitoring and analysis

Advanced processing requirements for capturing and processing

- High-bandwidth video
  → few FPS to 60FPS up to 4K (~MBps)
  → Typically USB (2.0, 3.0 and C)
  → Some (slower) via SPI/I2C

Zynq 7000-series

Raspberry PI

Coral TPU

- Array of microphones
  → PDM or I2S → datastream from 8kSps up to 96kSps (I2S) or up to ~5MSps PDM per microphone

USE CASES

HIGH-END SENSING PLATFORMS

Advanced processing requirements for capturing and processing

- Real-time local processing to avoid data congestion
- Local permanent storage (~Gbs up to ~Tbs)
- ~MB up to GB of required RAM
- Mid-and high-end embedded devices
- May run dedicated higher level operating system (e.g. embedded Linux)
- Heterogeneous architectures (Multi-core, System-on-Chip, TPUs, CPU + FPGA, etc.)

USE CASES

HIGH-END SENSING PLATFORMS

More stringent security requirements

- Minimally same security as low-end devices
- Secure permanent local storage
  → confidentiality of audio/video
- Secure (high-speed) data
  communication to server
- Protect against unauthorized access
  (e.g. ssh, console via UART)

MID- AND HIGH-END DEVICES AND PLATFORMS

ESP-32 SECURE PLATFORMS

ESP-32 SoCs (Espressif Xtensa LX7) do implement custom built-in security features/functions

- eFuse
- Encrypted flash
- Secure boot
- Firmware signature verification
- AES, SHA and RSA

MID- AND HIGH-END DEVICES AND PLATFORMS

INFINEON

Many implementations from low-end to high-end controllers

- AURIX tri-color (3-core) MCU based on RISC architecture
- PsoC ARM Cortex controller (M0/M0+/M3/M4) single or multi-core controllers
- PsoC-64 dual core: M0+ is used to establish a secure processing environment (SPE) while M4 is the non-secure counterpart (NSPE). IPC ensures communication between cores. Secure boot, attestation
- OPTIGA Trust: dedicated chips to address specific requirements
  → Product authentication / brand protection
  → Security in wireless charging
  → TPM
  → Connect for SIM-cards (IoT)
  → Authenticate for unique ID for “things”

NEXT STEPS

Selection of sensing hardware

Desired processing steps, compression, required bandwidths, etc.

Selection of appropriate processing platform to process sensory data

Storing and transmitting data to cloud

Thank you for your attention