



SPARTA

RIOT-FP DEMO

Feb. 28th 2020, Brussels

Emmanuel Baccelli
Inria

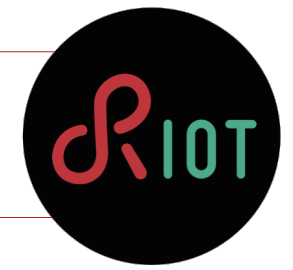
SECURE IoT SOFTWARE UPDATES



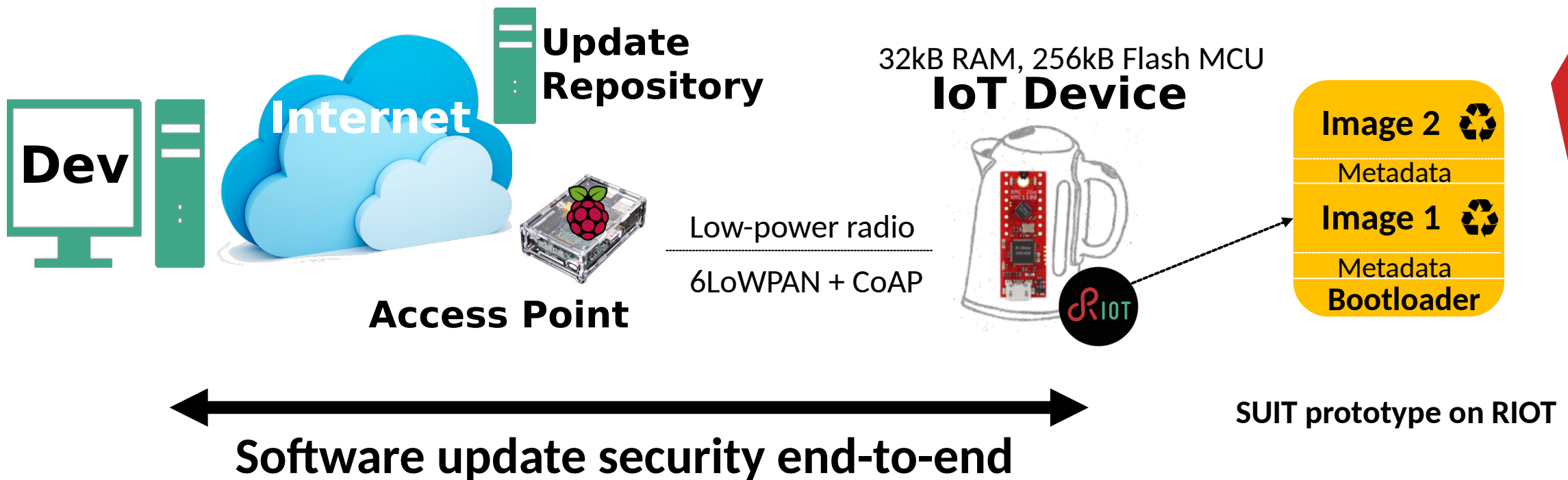
- What Internet-age software has taught us:
 - you can't secure what you can't update!
 - software updates are an attack* vector!
- ⇒ Enabling (legitimate) software updates is crucial & difficult
- ⇒ Even more challenging on microcontroller-based IoT devices

* www.wired.com/story/ccleaner-malware-supply-chain-software-security

RIOT-FP SECURE SOFTWARE UPDATE PROTOTYPE

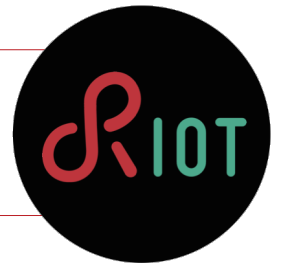


- We contribute to SUIT secure software update standardization at IETF (work-in-progress)
 - Architecture, metadata & crypto to guarantee authenticity & integrity of software updates
 - (see our work published in IEEE ACCESS*)



* K. Zandberg et al. "Secure Firmware Updates for Constrained IoT Devices using Open Standards: A Reality Check," IEEE Access, 2019.

DEMO! SUIT WORKFLOW ON RIOT



PHASE 0
Commission device

Maintainer (P,S)

(OOB: Provision Public Key P)

IoT Device

(Crypto: ed25519 digital signatures, SHA256 hash)

PHASE 1
Build update



[Image]

PHASE 2
Publish & sign update



[Manifest]

PUT Image, {Manifest}_s

Repo

GET

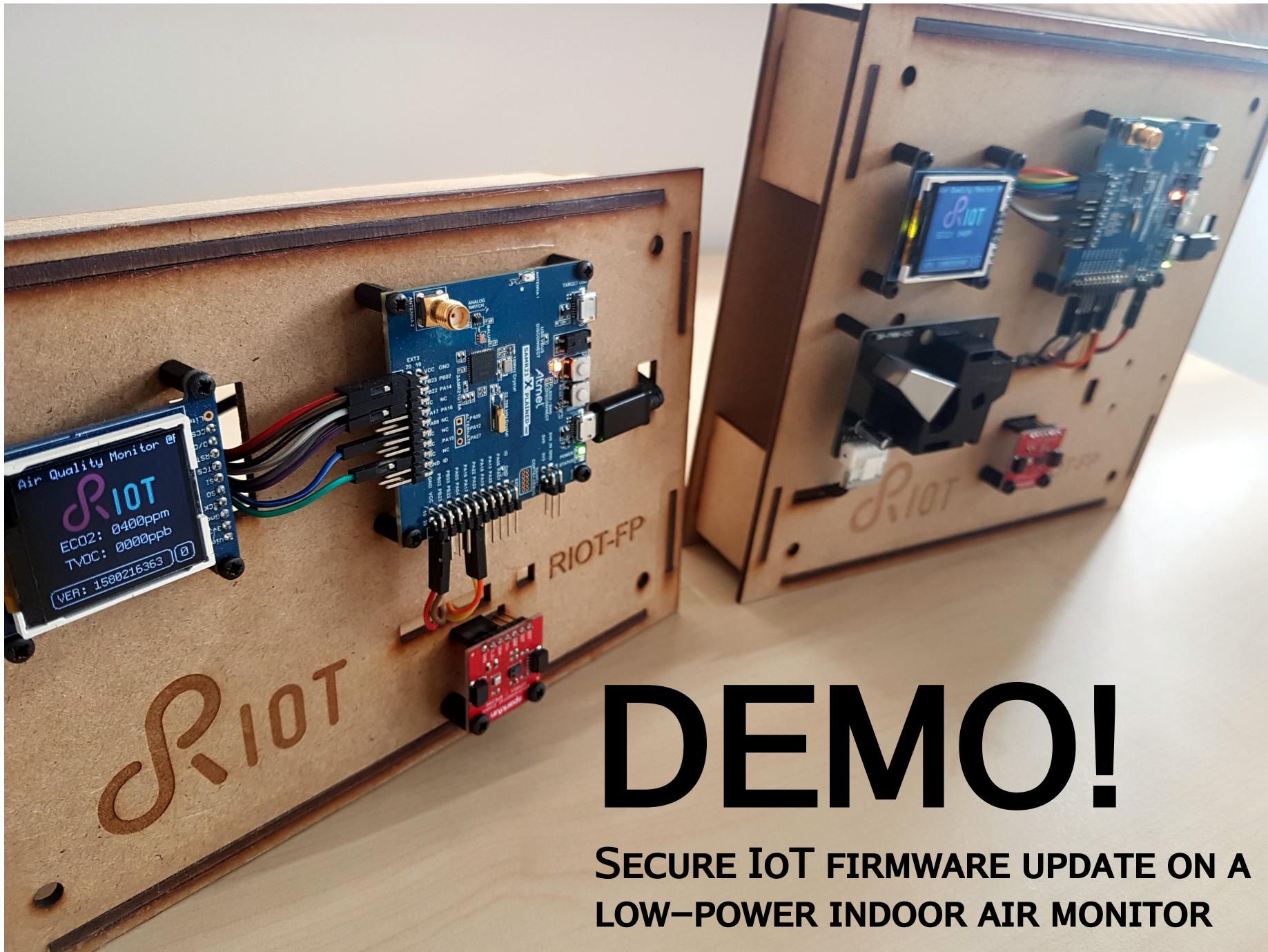
Device remains operational!

PHASE 3
Fetch update

PHASE 4
Auth.: check sign.
Integrity: check hash

PHASE 5
Check OK? Install.
(Else: send alert)





DEMO!

SECURE IoT FIRMWARE UPDATE ON A
LOW-POWER INDOOR AIR MONITOR





THANKS!

More on **RIOT** at github.com/RIOT-OS/RIOT
More on **RIOT-fp** at future-proof-iot.github.io/

