Aalto University

Secure Firmware Update for Resource Constrained Devices

Thomas Nyman, Aalto University & Trustonic

Software Update Landscape in IoT

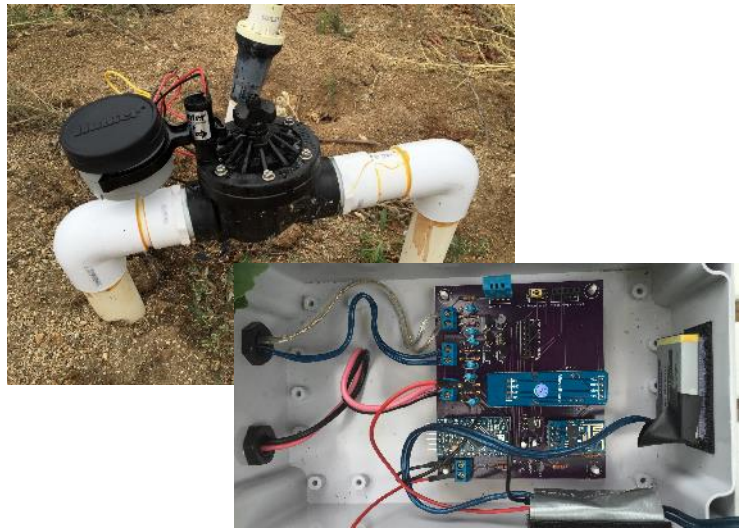
- **Security key concern for IoT, but adoption of security technology is lagging**
  - >80% of respondents in 2017 IoT Survey do not use Over-the-Air updates!

- **Even "*Secure by design*" devices have vulnerabilities discovered after deployment**
  - Software update enable fixes to bugs, but also introduction of new features

- **Existing update mechanisms not suitable for tiny IoT devices**
  - Existing solutions for microcontroller class devices ad hoc, often insecure

Eclipse Foundation IoT Developer Trends Survey 2017

Internet of resource constrained things



Solar-powered soil-moisture sensor for agricultural irrigation
https://hackaday.io/project/6444-vinduino-a-wine-growers-water-saving-project

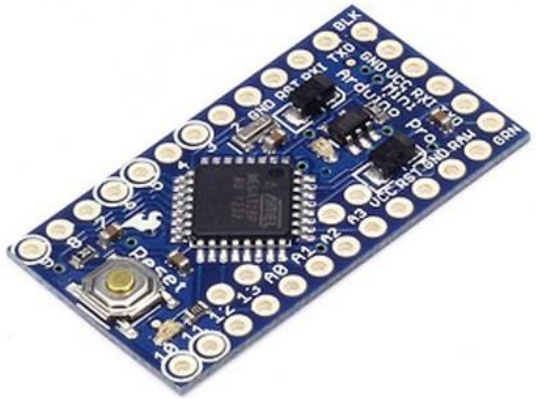
Wireless-enabled wearable activity tracker
https://en.wikipedia.org/wiki/Fitbit *(MorePix)*

Wireless vehicle-presence sensor with 7 to 10 years of battery life
http://embedded-computing.com/articles/sensor-enabled-nodes-support-the-iot-for-smart-buildings-and-smart-transport/

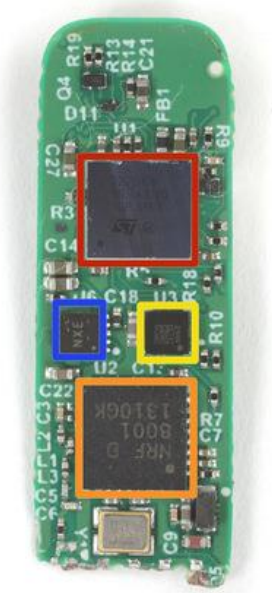
Remote-controlled consumer smart lighting platform
http://www.ikea.com/se/sv/catalog/categories/departments/lighting/36812/

Working horses for small IoT devices

ATmega328
Up to **16 MHz** Clock Speed
Up to **2 KB** SRAM
Up to **32KB** Flash
Up to **1 KB** EEPROM
Wifi + **Long range RF** (external)

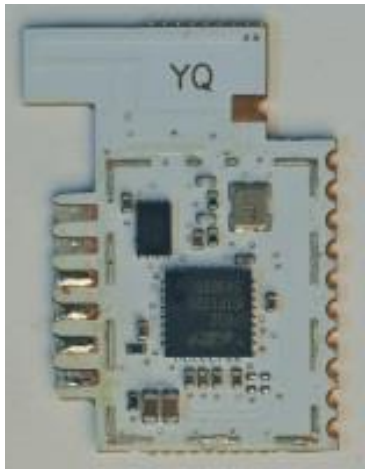


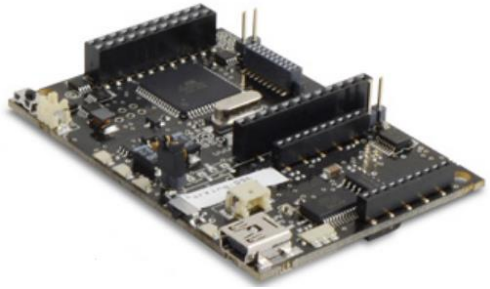
https://hackaday.io/project/6444-vinduino-a-wine-growers-water-saving-project
https://store.arduino.cc/arduino-pro-mini



ARM Cortex-M3
Up to **32 MHz** Clock Speed
Up to **16 kB** RAM
Up to **4kB** EEPROM
Up to **128 kB** Flash
Bluetooth LE

https://www.ifixit.com/Teardown/Fitbit+Flex+Teardown/16050
http://www.st.com/en/microcontrollers/stm32l151c6.html





ATmega1281
14.74 MHz Clock Speed
8 kB SRAM
4 kB EEPROM
128 kB Flash
ZigBee (external)

http://www.libelium.com/v11-files/documentation/waspmote/smart-parking-sensor-board_eng.pdf
http://www.libelium.com/products/waspmote/hardware/

ARM Cortex-M4 + Floating Point Unit
Up to **40 MHz** Clock Speed
Up to **256 kB** RAM
Up to **1024 kB** Flash
ZigBee and **Thread** Radio (6LoWPAN)
Hardware Crypto Accelerator w/
AES-256/128, ECC, SHA-1, SHA-2

https://www.heise.de/make/artikel/Das-steckt-in-Ikea-Tradfri-3597295.html
https://www.silabs.com/products/wireless/mesh-networking/efr32mg-mighty-gecko-zigbee-thread-soc

Characteristics of a *resource constrained* IoT system

- **Monolithic firmware written in embedded C/C++**
  - interrupt-driven, reacts to external events
  - at most simple real-time scheduling O/S (or no O/S at all!)

- **Execute-in-place from persistent storage (typically NOR flash)**
  - reduces total RAM requirements
  - flat memory space (no virtual memory)
  - access to memory controlled by Memory Protection Unit (MPU)

- **Limited processing power, storage and memory**
  - Restricted lifetime in battery operated devices

Software update for commodity devices

- **(Nearly) all code executes from RAM**
  - Copy in persistent storage can be freely replaced
- **Highly modular software architectures**
  - Components (apps, kernel, services) may be updated individually
- **Established software packaging and distribution mechanism**
  - Update- and code-signing

Characteristics of a *secure-by-design* IoT system

- **Root-of-Trust based in hardware**
  - foundation from which trust in integrity and security can be established
  - immutable except by authorized entities

- **Crypto-acceleration**
  - For securing remote communications

- **Hardware-enforced isolation between Trusted and Non-trusted software**
  - Secure architectures such as **SMART**, **TrustLite**, **TyTan** and **TrustZone-M**

TEE / Enclaves for MCUs

SMART: Secure and Minimal Architecture for (Establishing Dynamic) Root of Trust, ISOC Symposium on Network and Distributed System Security (NDSS), 2012.
TrustLite: a Security Architecture for Tiny Embedded Devices, European Conference on Computer Systems (EuroSys), 2014.
TyTAN: Tiny trust anchor for tiny devices, Design Automation Conference (DAC), 2015
TrustZone technology for ARMv8-M Architecture Version 1.1

Isolation breaks monolithic systems down into modular pieces

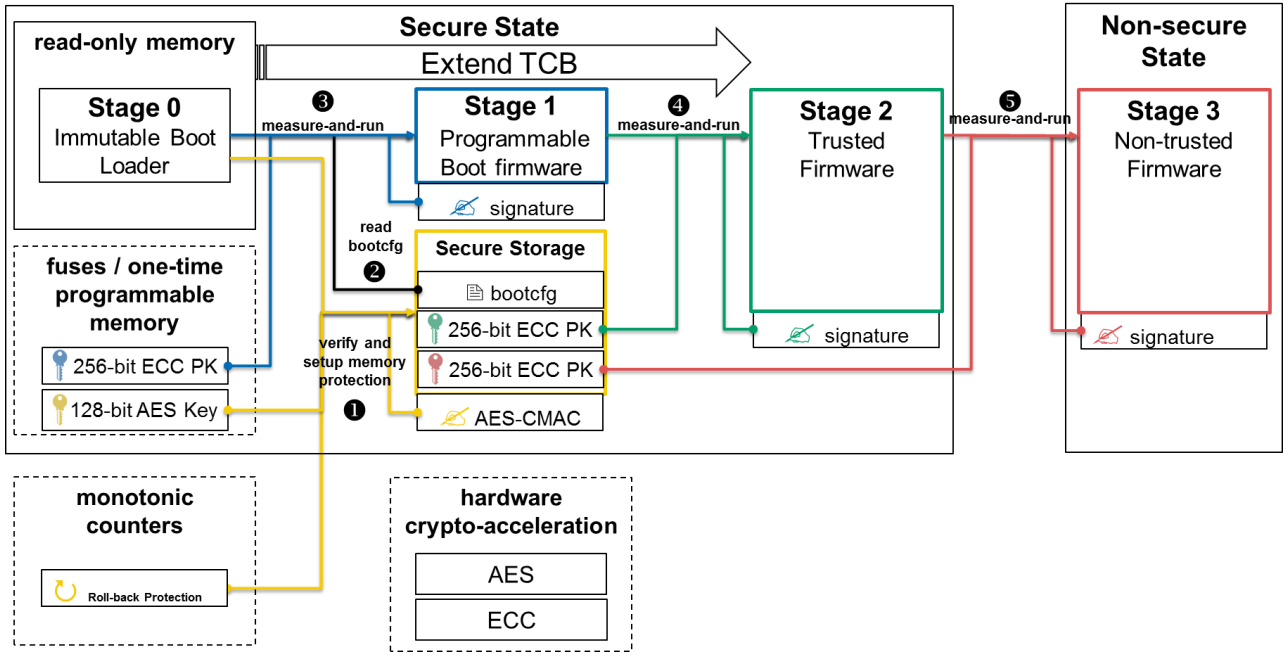
Firmware Update Requirements

- **Packaging for Over-the-Air delivery**
  - agnostic of specific communication stack
- **Secure, establishing integrity and authenticity of device firmware**
  - limited to lighweight cryptography available
- **Robust, but without assuming space for full copy**
  - retain ability to recover device after failed update
- **Verifiable, by remotely attesting success update process**
- **Efficient, minimize use of limited resources**

Activities in SELioT

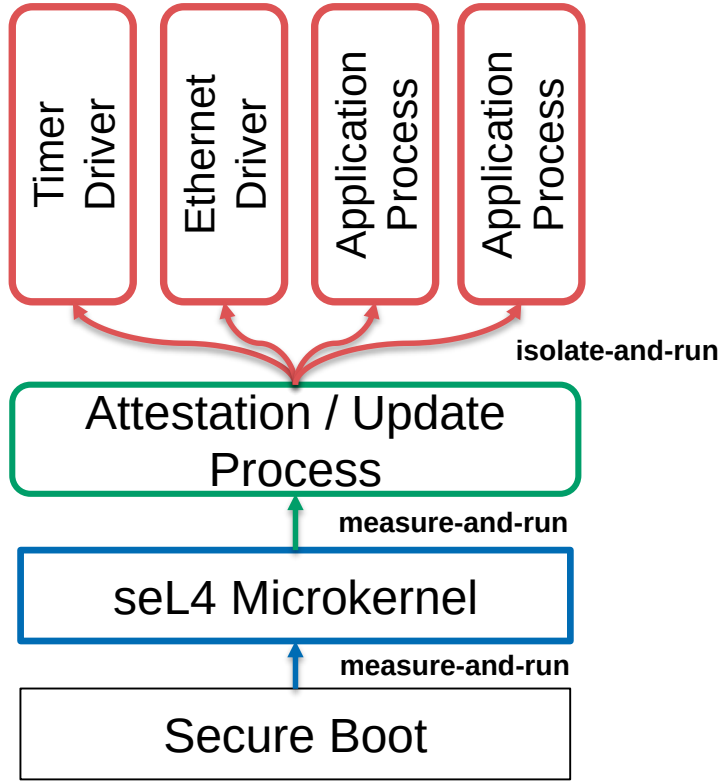
Aalto University

- Firmware update and secure boot co-design for MCUs with hardware-enforced isolation



UCI

- Attestation / Update with isolation through formally verified microkernel



Conclusion

- **Existing update mechanisms not suitable for tiny IoT devices**
  - Need to scale down to microcontroller-level

- **Strong isolation achievable even on tiny devices**
  - protect critical functionality
  - introduce modularity in monolithic systems