Measuring the Performance and Energy Cost of Cryptography in IoT Devices

- Hannes Tschofenig, Arm

Agenda

- Obtaining data about performance and power consumption about crypto on IoT devices is difficult.
- At IETF#95 I spoke about an effort to develop a benchmark.
- The first version of this benchmark is now available.

EMBC® EMBEDDED MICROPROCESSOR BENCHMARK CONSORTIUM

Organization developing benchmarks for processors and MCUs since the late ‘90s.

CoreMark®
An EEMBC Benchmark

CoreMark is a benchmark that measures the performance of CPU used in embedded systems.

EEMBC has established several working groups developing IoT benchmarks.

ULPMark™
An EEMBC Benchmark

IoTMark™-BLE
An EEMBC Benchmark

SecureMark™-TLS
An EEMBC Benchmark

SecureMark™-TLS
An EEMBC Benchmark

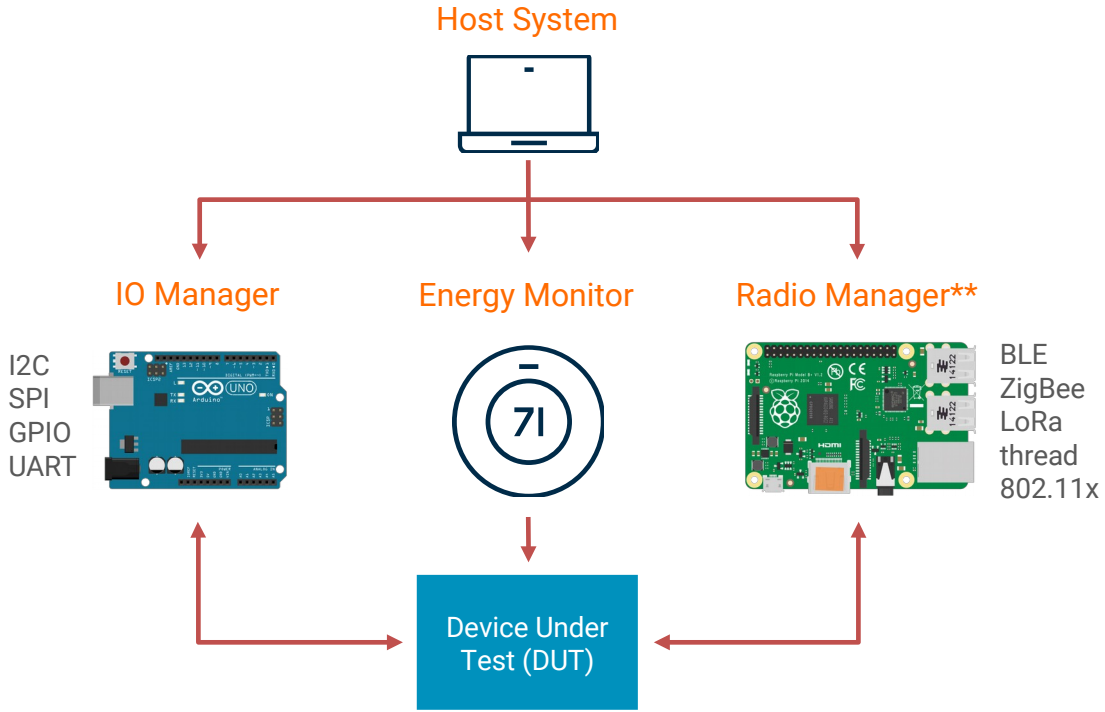
- SecureMark-TLS is a synthetic benchmark that models a TLS handshake without actually running the handshake. Starting point is the TLS_ECDHE_ECDSA_WITH_AES_128_CCM ciphersuite.
- It measuring the performance and power consumption.
- It does this using the IoTConnect framework: a physical test harness and a firmware API that enables a wide variety of energy and performance benchmarking capabilities
- The firmware API is generic enough to facilitate the use of different software and hardware implementations of cryptographic functions and primitives.
- The reference implementation uses Mbed TLS for crypto.
- Details available at https://www.eembc.org/securemark

The IoTConnect Framework

Extensible framework with wired and wireless interfaces, with a hardware setup cost of <US$200*

* Note, this is the cost of the hardware from 3rd parties (e.g., Digikey, Farnell). Host software and DUT benchmark firmware licensed separately from EEMBC directly.

** Radio manager not required for SecureMark or ULPMark



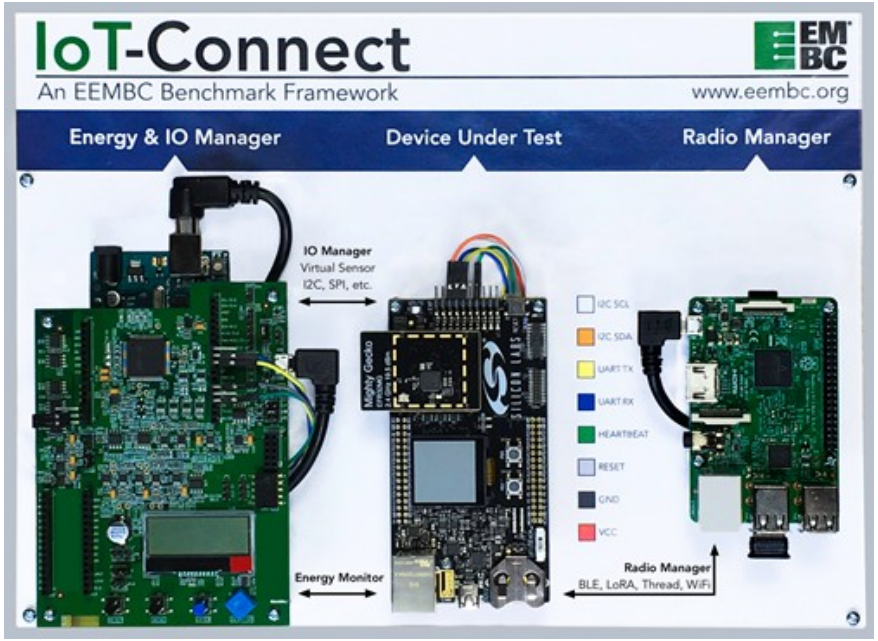
Actual Hardware Setup

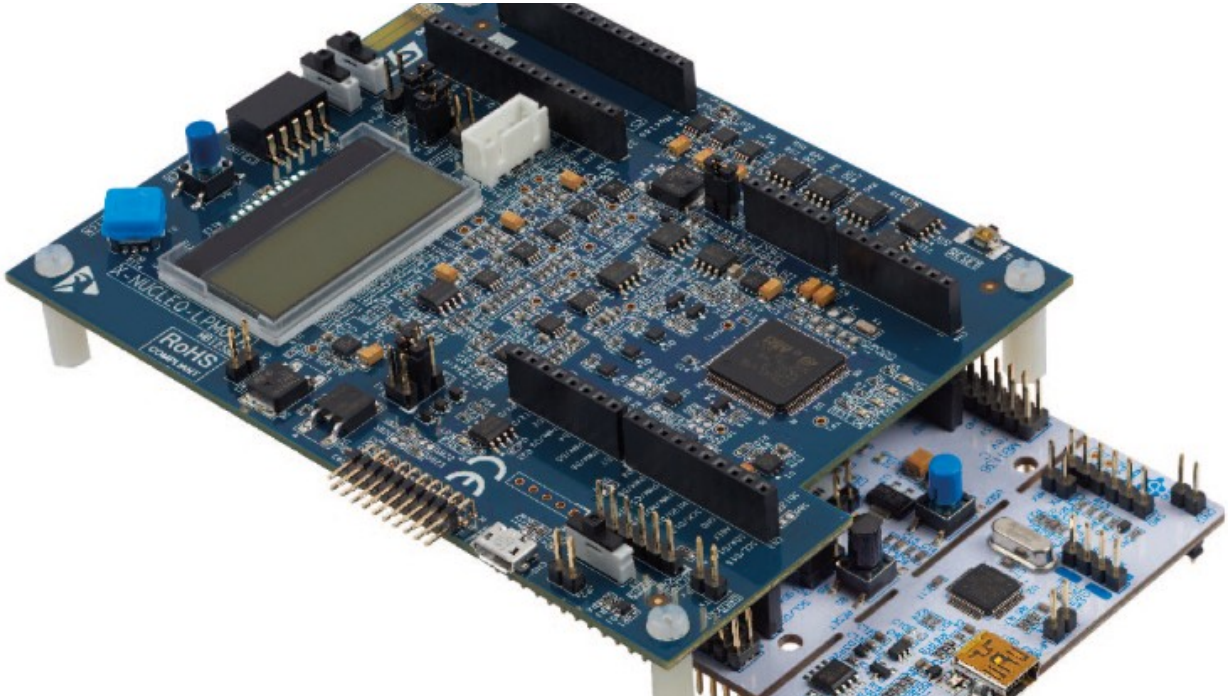
The DUT (center) is powered by the energy monitor (left).

The IO Manager (left, under EMON) acts as both sensor emulation and communication proxy.

The Radio Manager (right) acts as the wireless gateway (not needed for SecureMark)

The Host (not shown) coordinates all four subsystems.



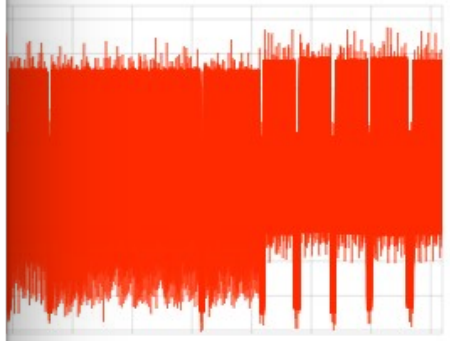


STM32 Power Shield - [X-NUCLEO-LPM01A]

Benchmark

- Single digit number +
- Detailed data

AES128 ECB Encrypt [144B]	8.02 uJ	179 us	44.7 mW
AES128 ECB Encrypt [224B]	11.7 uJ	261 us	44.7 mW
AES128 ECB Encrypt [320B]	16.1 uJ	360 us	44.7 mW
AES128 CCM Encrypt [52B]	14.8 uJ	340 us	43.6 mW
AES128 CCM Decrypt [168B]	28.8 uJ	656 us	43.8 mW
ECDH p256r1 Secret Mix	20.7 mJ	485 ms	42.7 mW
ECDSA p256r1 Sign	8.58 mJ	201 ms	42.6 mW
ECDSA p256r1 Verify	29.1 mJ	681 ms	42.7 mW
SHA256 [23B]	1.51 uJ	35.1 us	43.1 mW
SHA256 [57B]	3.69 uJ	85.5 us	43.2 mW



Reset Zoom [301.9, 38.44]

Timestamps

```
t]: m-aes128_ecb-message-length-2048
-lap-us-337966000
t]: m-aes128_ecb-decrypt-start
-lap-us-348879000
t]: m-aes128_ecb-decrypt-finish
t]: m-ready
d #38 succeeded
g command #39: emon disable-timer (Timeout: 10s, #
-ready
```

Creating and Submitting SecureMark-TLS Scores

The first published SecureMark-TLS scores!

https://www.eembc.org/securemark/scores.php

Clear	Vendor	Device	Core	Core MHz	Core Vcc	Crypto Library	Certified	Score	Date ▼
☐	STMicroelectronics	STM32L562 Rev A	Cortex-M33	24	1.8	MBed TLS 2.4.2	✓	27400	2018-10-15
☐	STMicroelectronics	STM32L476RG Rev 4	Cortex-M4	24	1.8	mbedTLS 2.4.2	✓	4220	2018-09-25

Detailed results include information about

- Compiler, linker, and toolchain
- Crypto library (mbedTLS 5.4.0) plus security-relevant optimizations, and
- Detailed energy and performance subscores for AES ECB Encrypt, AES CCM Encrypt/Decrypt, ECDH p256r1, ECDSA p256r1 Sign & Verify, and SHA256.
  - For example: The ECDSA sign operation takes 438 msec and the verify operation needs 1500 msec

Summary

- With SecureMark-TLS we created the first IoT security benchmark.
- It will help developers and designers to know upfront what performance and power consumption to expect from a given MCU for state-of-the-art crypto
  - High level score available for easy comparison
  - Detailed data within the disclosure form
- Features of SecureMark-TLS v2 under discussion.
- EEMBC is ready to receive score submissions.