EEMBC IoT Security Benchmarks

Hannes Tschofenig
(hannes.tschofenig@arm.com)
IoT Devices cannot do crypto, right?

• Wrong!
• Looked at the performance of various state-of-the-art crypto operations on MCUs.
  – Presented the investigations in the LWIG working group.
  – Provided input to the 2015 NIST workshop on lightweight cryptography.
• Hope was that others (e.g., researchers) help analyse the performance on other MCUs and do additional tests.
Some time later...

- Unfortunately, we had to realize that most researchers care more about inventing new algorithms than analysing existing algorithms on available hardware.
- We cannot run the tests on the wide range of MCUs from different vendors ourselves.
- A dead end?
It turns out that there is an organization that develops benchmarks for processors and MCUs and has been doing this since the late ’90s.

– For example, CoreMark is a synthetic benchmark that measures the performance of CPU used in embedded systems.

EEMBC has established groups working on benchmarks for IoT, which are called IoT-Connect, IoT-Secure and IoT-Gateway.
IoT Security Benchmark

• Measurements:
  – Performance
  – Energy Efficiency
  – Memory

• Tests have to work with different crypto implementations and with hardware from different vendors.

• Initial selection is based on AES, SHA256, ECDH, ECDSA.

• Group writes code for the tests and reference implementation uses mbed TLS crypto, libTomCrypt, and microECC.
Test Setup

• Test setup re-used from IoT-Connect benchmark (but without radio manager).
Upcoming Work

• To provide a synthetic benchmark we are investing the use of TLS/DTLS 1.2.
• The idea is to take the performance of the individual cryptographic operations of common cipher suites and to sum them up.
  – Starting point is TLS_ECDHE_ECDSA_WITH_AES_128_CCM
  – This should approximate the cryptographic performance of the handshake (without taking packet parsing and network transmissions into account).
  – No real handshake actually executed.
• We will compare the approximation with real world exchanges to determine the difference.
Looking Forward

• Will add other implementations and other algorithms as well. Feedback and input appreciated.

• Get in touch with us if you have experience with benchmarks and IoT security performance testing?

• Could share info on the SAAG list as we make progress (if there is interest).
Questions?
Contact Information

• IoT-Secure Benchmark Working Group Chairs:
  – Mike Borza (Mike.Borza@synopsys.com)
  – Ruud Derwig (Ruud.Derwig@synopsys.com)

• EEMBC President
  – Markus Levy (markus.levy@eembc.org)