RIOT at IETF Hackathon 115

Leandro Lanzieri, Martine Lenders, José I. Álamos, Koen Zandberg,
Emmanuel Baccelli, Lena Boeckmann, Lasse Rosenow, Bennet Blischke

PSA* Crypto in RIOT

- Problem: Persistent key storage using PSA
  - Working PoC
  - AES key can be stored in flash memory
- Problem: Integration of additional crypto backends
  - Working PoC with StSafeA secure element (SE)
  - Switching between SEs of different types
- Problem: Automatic selection crypto backends depending on hw capabilities
  - Integration into build system
  - With Kconfig and Makefiles
- Problem: Integration of PSA Architecture Testsuite
  - Integration of tests as package in RIOT

*Platform Security Architecture

IPv6 support over IEEE 802.15.4e DSME using 6LoWPAN

- Working implementation
- Review process for merging has started

RIOT (libSCHC) / OpenSCHC plugtest

Preparations (Saturday)

- CoAP compression rule handling still needs work on both sides

libSCHC	OpenSCHC
Mappings with offset (e.g. CoAP type)	ETag & Block-wise option compression
Compressing >1 URI components	

- Agreeing on a common SCHC rule set for the plugtest:
  - IPv6/ICMPv6/UDP
  - Values based on RIOT Release specifications

Plugtest (Sunday)

- **Issues in parsing/compressing ICMPv6 messages fixed**
- **CORECONF needed for routing/neighbor configuration**

CORECONF in RIOT

- Working implementation:
    - Discovery of available modules missing
- Problem: What is mandatory to implement
    - Refer to RESTCONF spec
- Problem: How to discover capabilities of the constrained device
    - RESTCONF has a mechanism
    - Not available in CORECONF
    - Discussion: Carry over RCMON (rfc8040) over to CORECONF?
- Future work:
    - Pull request it to RIOT!