Berlin SUIT Hackathon - Participants

- Henk Birkholz (Fraunhofer)
- Jan-Frederik Rieckers (Fraunhofer)
- Francisco Acosta (Inria)
- Anton Gerasimov (HERE Technologies)
- Brendan Moran (Arm)
- Hannes Tschofenig (Arm)
- Matthias Waehlisch (FU Berlin)
- Koen Zandberg (Inria / FU Berlin)
- Max Gröning (Texas Instruments)
- Emmanuel Baccelli (Inria)
- Daniel Petry (FU Berlin)
- Gaetan HARTER (FU Berlin)
- Carsten Bormann (Uni Bremen TZI)
- Markus Gueller (Infineon) - remote
- Ralph Hamm (Infineon) - remote
- Frank Audun Kvamtrø (Nordic Semiconductor) - remote
- Øyvind Rønningstad (Nordic Semiconductor) - remote
- Milen Stoychev (Ackl.io) - remote
- Fabio Utzig (Apache) – remote
- David Brown (Linaro) – remote

SUIT-compliant IoT firmware updates!!

IoT Hackers!!

repo.riot-labs.de/files

repo.riot-labs.de/files

firmware or manifest: Choisir un fichier Aucun fichier choisi submit

	name	SHA1 truncated	size
○	test-file-payload.json	c860495c8e167802	789B
○	cladmi_kYc0o_slot2.bin	58c040da72a9e213	70112B
○	djp_mf_3_orig.cbor	56bc2b0b7940e02c	207B
○	djp_mf_1_orig.cbor	697d8b35f2714fa2	189B
○	djp_2_update_slot2.bin	4a8d174f184846ad	70600B
○	cladmi_kYc0o_private.key	57d9fe061c47b314	64B
○	test-oytis-raw-payload.cbor	30675ccc41cfd687	227B
○	cladmi_kYc0o_slot2.manifest.2	841ed9e95cdc4b4e	205B
○	cladmi_kYc0o_slot2.manifest	6747bb960f6bd20b	205B
○	test.cbor	427f4ef761705fb0	259B
○	djp_1_orig_slot2.bin	731c693eb00d09c4	70096B
○	djp_mf_4_update.cbor	e558eada1259070f	207B
○	djp_mf_2_orig.cbor	272f7e7b65b3669c	191B
○	iotlab-m3_suit_updater-slot2.bin	0d33f6e364bf4983	68376B
○	iotlab-m3_suit_updater-slot2.manifest	76aaf4e73fea5059	205B
○	djp_2_incrcoapbuf_slot2.bin	8ea9e7e93a5c6379	70608B
○	djp_mf_5_incbufsize.cbor	177e433f1feb6392	207B

CoAP URL coap://target.host/local/

Cose signed ☐

submit

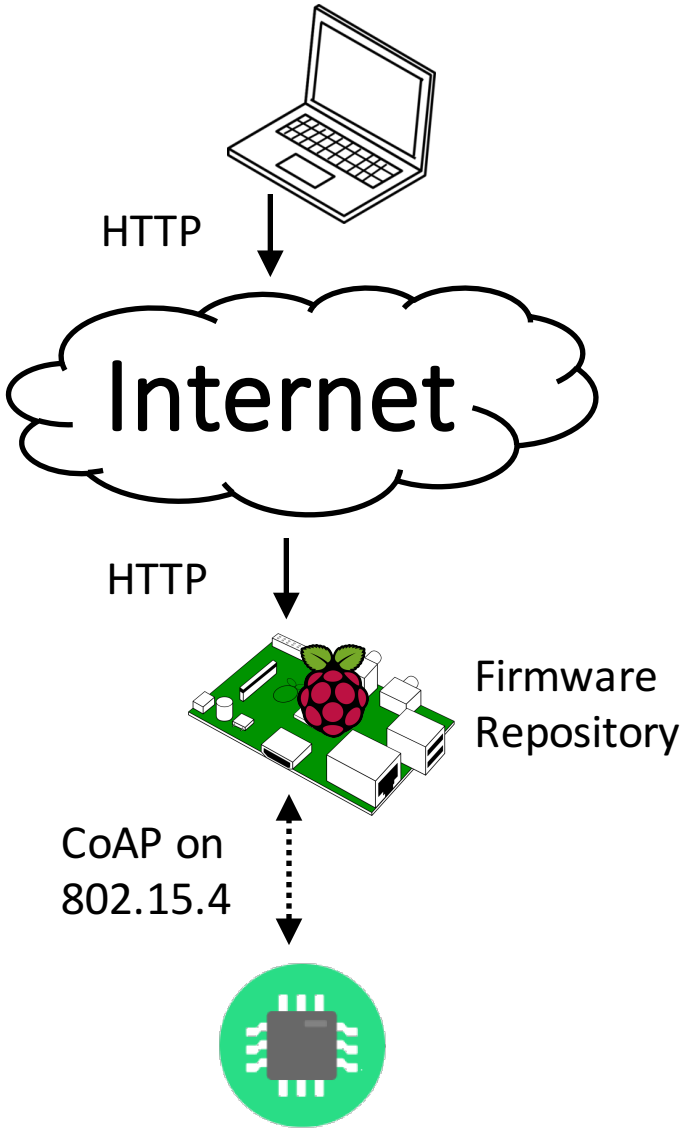
Implementation & Tests at SUIT Hackathon

(Koen, Gaëtan, Paco, Dan, Matthias, Emmanuel + help of Kaspar)

- **Manifest parser implementation**
  - Implementation, compliant with current spec
  - Standalone COSE implementation (libcose)
- **Successful end-to-end test(s)**
  - Generate firmware + signed SUIT manifest
  - Upload manifest + firmware to shared repo
  - Download manifest + firmware on device
  - Verification and boot update on RIOT device

Atmel SAMR21
Cortex-M0+
32kRAM, 256kROM

STM32 (IoT-Lab)
Cortex-M3
64kRAM, 512kROM



Group working with Mbed OS

(Brendan, Hannes, Max with help from Koen)

- We used the K64F board for our experiments
- Migration from Arm internal COSE library to the open source libcose implementation, which utilizes Mbed TLS.
- libcose is compiling without errors on the K64F board.
- Verification of COSE-protected manifest worked after problems with the raw public key handling got resolved.
  - We incorrectely used the Mbed TLS APIs for importing the ECC keys.
  - We noticed that the RIOT group used a signing algorithm not supported by Mbed TLS (namely ed25519).

CDDL Specification Learning

(M. Gueller, R. Hamm)

- Focus on CDDL Specification for a Minimalistic COSE Crypto Container COSE_Sign Profile
- Goals:
  - Get Familiar with CDDL Specification for SUIT Crypto Container
  - Get Familiar with Tool generating Diagnostic CBOR Instances based on CDDL Specification
- Achievements
  - Created Minimalistic COSE_Sign CDDL Specification (including Key ID, Algorithm Header and 1 Signature). This was based on COSE Profile for Coswid
  - Run through CDDL Tool and generated several CBOR Instances
- Next Steps
  - Experts Review?, Basis for COSE_Encrypt,…

Resources

- SUIT generator
  - Manifest generator (version: https://tools.ietf.org/html/draft-moran-suit-manifest-01)
  - https://github.com/ARMmbed/suit-manifest-generator
  - NOTE: https://github.com/ARMmbed/suit-manifest-generator/pull/3 adds tool for converting PEM files to x/y points as used by libcose+mbedtls
- libcose on GitHub:
  - https://github.com/bergzand/libcose
- Setup for common SUIT repo infrastructure
  - https://github.com/suit-wg/Hackathon-Interim-Berlin/wiki/Interop-Setup
- Online CBOR parsers
  - http://cbor.me/
  - https://geraintluff.github.io/cbor-debug/
- WIP libcose integration with mbed:
  - https://github.com/suit-wg/mbed-libcose
- libcose integration with RIOT-os:
  - https://github.com/bergzand/RIOT/blob/app/suit-ota/sys/firmware/firmware_manifest.c#L228
- WIP SUIT parser in RIOT-os:
  - https://github.com/bergzand/RIOT/blob/app/suit-ota/sys/suit/suit.c

Etherpad with more info (raw)

https://pad.inria.fr/p/cYawtv2ivnoOl60X_suit-hackathon