IETF Hackathon: Software / Firmware updates for IoT devices

IETF 111
July 19-23, 2021
Online
Hackathon Plan

1. Get the software/firmware to the device
   - Constrained IoT devices: LwM2M with OSCORE security for CoAP
   - Regular IoT devices: TEEP for trusted app update on TEE

2. Secure the update using the SUIT manifest

3. Use the new software/firmware

Three teams with sync-points between them.
What got done

- Identified issues with the TEEP protocol
  - [https://github.com/ietf-teep/teep-protocol/issues](https://github.com/ietf-teep/teep-protocol/issues)

- Integration of OSCORE into Leshan (LwM2M server) and Wakaama (LwM2M client) (in progress)
  - Successfully tested registration with the Wakaama client to the Leshan server using OSCORE
    - [https://github.com/leandrolanzieri/RIOT/tree/pkg/wakaama/add_oscore](https://github.com/leandrolanzieri/RIOT/tree/pkg/wakaama/add_oscore)
    - [https://github.com/eclipse/leshan/tree/oscore](https://github.com/eclipse/leshan/tree/oscore)

- SUIT integration in Mcuboot (in progress)
  - Update of the SUIT manifest generator: [https://gitlab.arm.com/research/ietf-suit/suit-tool](https://gitlab.arm.com/research/ietf-suit/suit-tool)
  - Update of the libcsuit parser: [https://github.com/yuichitk/libcsuit](https://github.com/yuichitk/libcsuit)
struct image_header {
    uint32_t ih_magic;
    uint32_t ih_load_addr;
    uint16_t ih_hdr_size;
    uint16_t ih_protect_tlv_size;
    uint32_t ih_img_size;
    uint32_t ih_flags;
    struct image_version ih_ver;
    uint32_t _pad1;
};
SUIT and Mcuboot
Investigating the best integration options

- New magic number
- Manifest size included.

Software:
- Libcsuit (for manifest parsing)
- QCBOR (for CBOR parsing)
- T_cose (for COSE parsing)
- Mbed TLS with PSA Crypto API
- Separate code for HPKE and AES-KW (firmware encryption)

Looking also into Brendan’s library, which uses uECC and Mbed TLS (for SHA256)
What we learned at this hackathon

• Great interactions despite online nature of the event and the timezone differences
• Regular work disturbs the “flow” and our plan was a bit too ambitious …
• Secure bootloaders are more complex than they might appear. Bootloader testing is different than protocol testing.
• Thanks to Matt Gillmore for suggesting the LwM2M theme. Was a good way to work with new people.
Wrap Up

Team members:
• Dave Thaler (TEEP)
• Brendan Moran (SUIT)
• Leandro Lanzieri (OSCORE)
• Rikard Höglund (OSCORE)
• Hannes Tschofenig (SUIT)
• David Brown (Mcuboot)

With help from
• Daniel Innes (LwM2M)
• Simon Bernard (LwM2M)
• Achim Kraus (LwM2M)
• Akira Tsukamoto (TEEP)
• Isobe Kohei (TEEP)
• Kikuchi Masashi (TEEP)
• Takahiko Nagata (TEEP)
• Ken Takayama (TEEP)

First timers @ IETF/Hackathon: Leandro