IETF Hackathon:
Software / Firmware updates for IoT devices

IETF 111
July 19-23, 2021
Online

Hackathon Plan

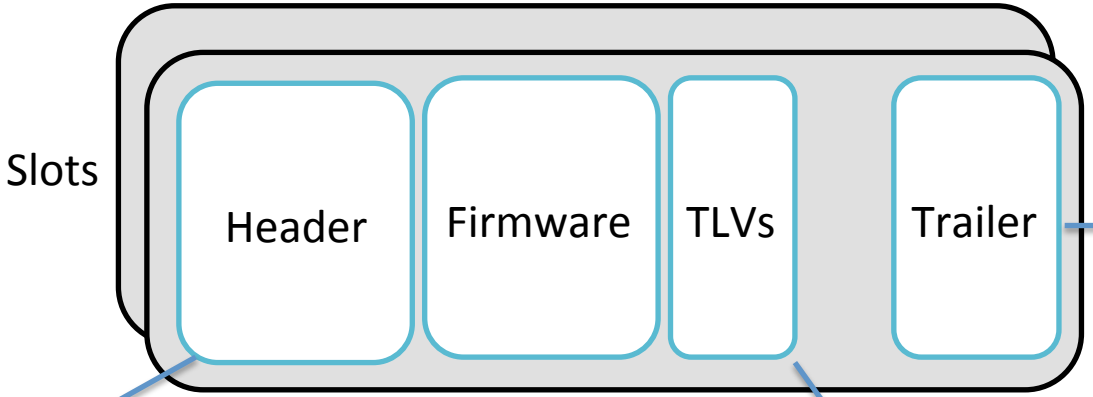
1. **Get the software/firmware to the device**
   - Constrained IoT devices: LwM2M with OSCORE security for CoAP
   - Regular IoT devices: TEEP for trusted app update on TEE
2. **Secure the update using the SUIT manifest**
3. **Use the new software/firmware**

Three teams with sync-points between them.

What got done

- Identified issues with the TEEP protocol
  - https://github.com/ietf-teep/teep-protocol/issues
- 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/eclipse/leshan/tree/oscore
- SUIT integration in Mcuboot (in progress)
  - Simulator preparation: https://github.com/mcu-tools/mcuboot/tree/suit-111
  - Update of the SUIT manifest generator: https://gitlab.arm.com/research/ietf-suit/suit-tool
  - Update of the libcsuit parser: https://github.com/yuichitk/libcsuit

MCUboot



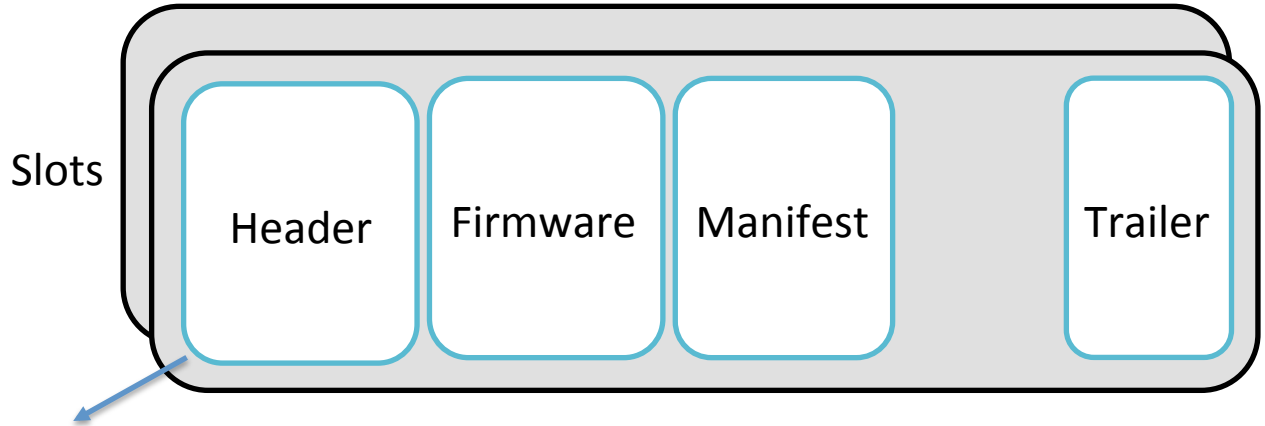

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                                                               ~
~    Swap status (BOOT_MAX_IMG_SECTORS * min-write-size * 3)    ~
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Encryption key 0 (16 octets) [*]               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Encryption key 1 (16 octets) [*]               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Swap size (4 octets)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Swap info   |           0xff padding (7 octets)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Copy done   |           0xff padding (7 octets)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Image OK    |           0xff padding (7 octets)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      MAGIC (16 octets)                        |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```c
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;
};
```

```c
#define IMAGE_TLV_KEYHASH          0x01   /* hash of the public key */
#define IMAGE_TLV_SHA256           0x10   /* SHA256 of image hdr and body */
#define IMAGE_TLV_RSA2048_PSS      0x20   /* RSA2048 of hash output */
#define IMAGE_TLV_ECDSA224         0x21   /* ECDSA of hash output */
#define IMAGE_TLV_ECDSA256         0x22   /* ECDSA of hash output */
#define IMAGE_TLV_RSA3072_PSS      0x23   /* RSA3072 of hash output */
#define IMAGE_TLV_ED25519          0x24   /* ED25519 of hash output */
#define IMAGE_TLV_ENC_RSA2048      0x30   /* Key encrypted with RSA-OAEP-2048 */
#define IMAGE_TLV_ENC_KW           0x31   /* Key encrypted with AES-KW-128 or
                                             256 */
#define IMAGE_TLV_ENC_EC256        0x32   /* Key encrypted with ECIES-P256 */
#define IMAGE_TLV_ENC_X25519       0x33   /* Key encrypted with ECIES-X25519 */
```

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)

First timers @ IETF/Hackathon: Leandro

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)