FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

DIE HOCHSCHULE, DIE MEHR KANN.

# Secure Firmware Updates Over the Air in the IoT

IT-SECURITY MASTER

# Riot-OS Summit
# Secure Firmware Update OTA

Vienna 2024

Miguel Arcilla, Silvie Schmidt

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES


> **Miguel Arcilla**

> Graduate Student in IT-Security Master @ FH Campus Wien

  > miguel.arcilla@stud.fh-campuswien.ac.at

> Software Engineer @ Porsche Informatik GmbH


> Bachelor Thesis:

  > Secure Update Processes for the Internet-of-Things

  > Focus on firmware encryption

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES


> **Silvie Schmidt**
> Academic Staff; City of Vienna Endowed Professorship for IoT-Security
> Research Centre for IT-Security, Master's Degree Program IT-Security
> silvia.schmidt@fh-campuswien.ac.at


Vienna 2025
IT-S NOW
Listen. Learn. Act.
Powered by FH Campus Wien
www.its-now.science?conference

> **Organisation Conference IT-S NOW!**
> https://its-now.science

> ***Head of ELVIS – Embedded Lab for IoT & Security***
> https://elvis.science

ELVIS
EMBEDDED LAB VIENNA FOR IOT & SECURITY

> ***Campus Cyber Security CTF-Team***
> https://www.campus-cybersecurity.team/

Cyber Security Team
FH Campus Wien

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

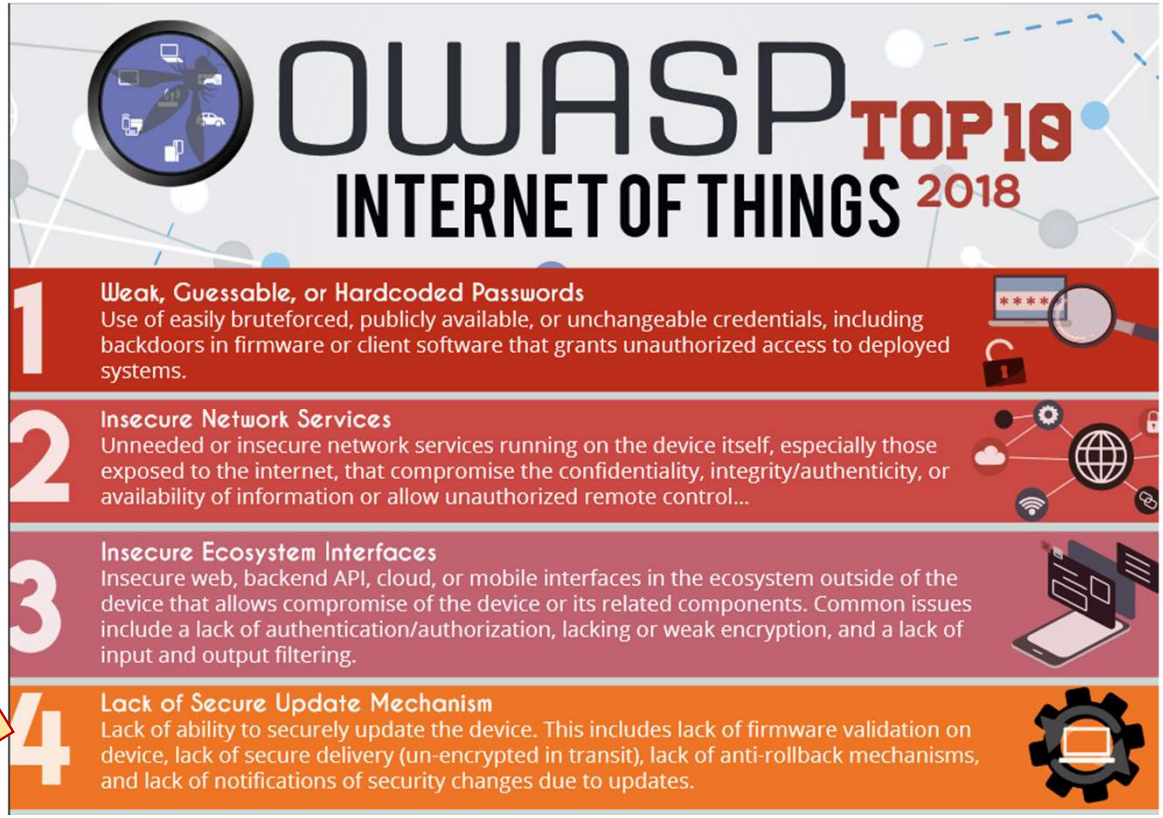
# The Firmware Update Process ….

> …is crucial in the Internet of Things

> …and one of the most critical processes


[23]

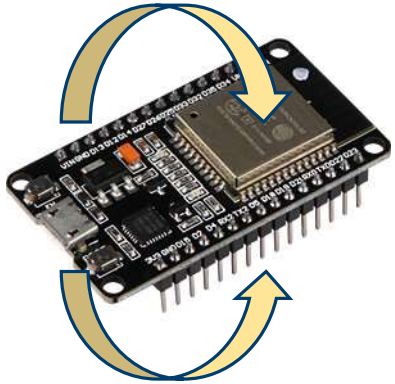
[21]



FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Definitions

- Constrained devices:
  - no common OS - embedded OS, e.g. Contiki, RIOT-OS,…
  - often no OS at all



- Firmware:
  - IEEE: combination of HW & SW
  - Often: either exclusively HW or SW
  - In this talk: application that runs on the device (SW)

- FOTA: Firmware update over the air
- SFOTA: Secure FOTA

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Definitions

> Cryptographic Objectives

> Confidentiality
> Integrity
> Authenticity
> Non-Repudiation

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Threats

> ***What can go wrong?***

- > Wrong firmware
- > Bad firmware
- > Power failure
- > Transmission errors
- > Not working firmware
- > And many more….

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Threats

> ***Update Process Safety Issues***

> *Transmission Error*

> *Transmission Failure*

> *Information Loss*

[3]

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Threats

> ***Update Process Security Issues***

> *Unauthorized Device*

> *Third-Party Firmware*

> *Altered Firmware*

> *Reverse-Engineering*

[3]

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

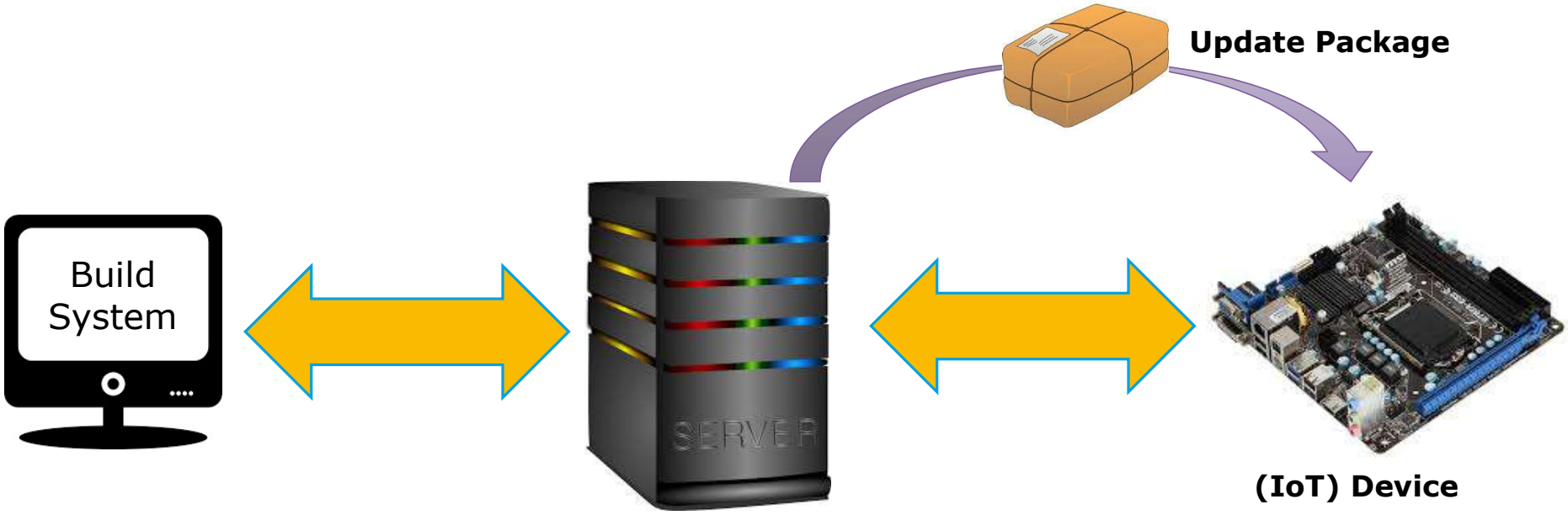
# Requirements

> ***Main Requirements for a Secure FW Update***

- Security
  - If the FOTA is insecure the device is insecure!
- Robust
- Atomic
- Fail-safe
- Remote management
- Auditable
- User data preservation

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Security Challenges




**Firmware Management Server**

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Considerations

- > ***RFC 9019***
- > *Example Firmware Update Decisions*

| Decision | Information Elements |
|---|---|
| Should I trust the author of the firmware? | Trust anchors and authorization policies on the device |
| Has the firmware been corrupted? | Digital signature and MAC covering the firmware image |
| Does the firmware update apply to this device? | Conditions with Vendor ID, Class ID, and Device ID |
| Is the update older than the active firmware? | Sequence number in the manifest (1) |
| When should the device apply the update? | Wait directive |
| How should the device apply the update? | Manifest commands |
| What kind of firmware binary is it? | Unpack algorithms to interpret a format |
| Where should the update be obtained? | Dependencies on other manifests and firmware image URI in the manifest |
| Where should the firmware be stored? | Storage location and component identifier |

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Security

> ***Conclusion – for now***

> In general, stronger security results in weaker performance!

> Basis for trade-off: application scenario

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Firmware Integrity

> ***Most used security feature***

> Often the only implemented security feature

> Integrity techniques solve many security issues

> BUT not everything is solved

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Firmware Update Strategies

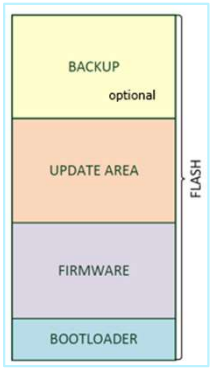
> In general, a FOTA in the Internet-of-Things (IoT) is done by replacing the full firmware at once (for simplicity reasons).

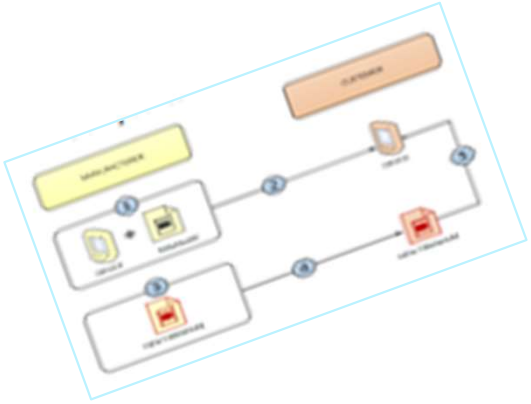
> Nevertheless, there are more options, i.e. strategies.

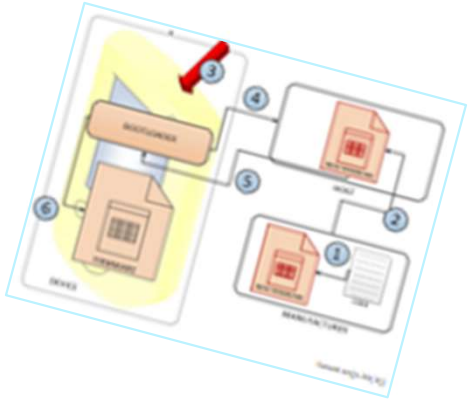
FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Conclusion for FWU Strategies

> Secure FW updates in the IoT are not trivial





FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# IoT Device Management

> ***Open Source Standards for Remote IoT Device Mgmt***

- > LWM2M[16]
- > CoMI[17]
- > OCF[18]
- > TR69 protocol[19]

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Firmware Update Frameworks

> SUIT – IETF working group for SW updates in the IoT (successor of FOSE)[13]
> Uptane, TUF – FWU for connected cars[11,7]
> MCUboot – FOTA for ESP8266 uCs[6]
> ReLog, Mate – using miniature VMs [8,9]
> CHAINIAC – blockchain-based [14]
> SWUpdate – mainly considered as a framework[15]
> ….Yocto.Mender.UpdateHUB.Z-Stack OTA.LWM2M…and many more

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Firmware Update Frameworks

> ***SUIT*** – SW Updates in the IoT

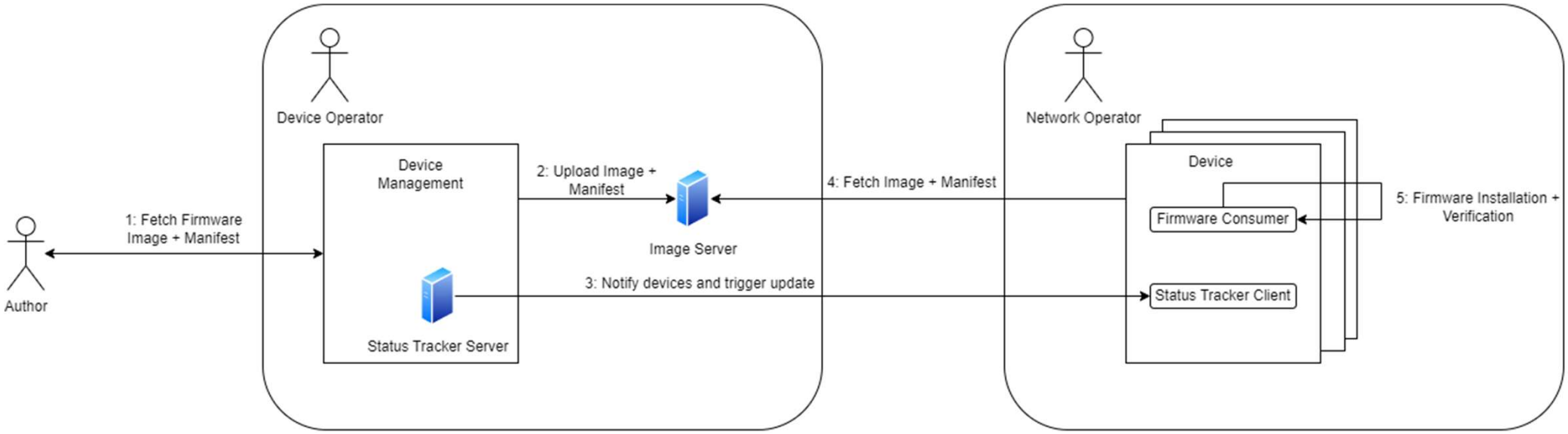
- > IETF working group
- > RFC 9019
- > Simple back-end architecture
- > Authentication & integrity protection
- > Encryption of FW image
- > Secure, even when updates are stored on untrusted repositories

[13]

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Firmware Update Frameworks

> ***SUIT*** – SW Updates in the IoT




Based on [13]

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Firmware Update Frameworks

- ***SUIT*** – SW Updates in the IoT
  - State-of-the-art security mechanisms
    - Mandatory-to-implement set of algorithms with at least keylengths of
      - 112-bit for symmetric cryptography
      - 233-bit for ECC cryptography
      - 2048-bit for RSA

[13]

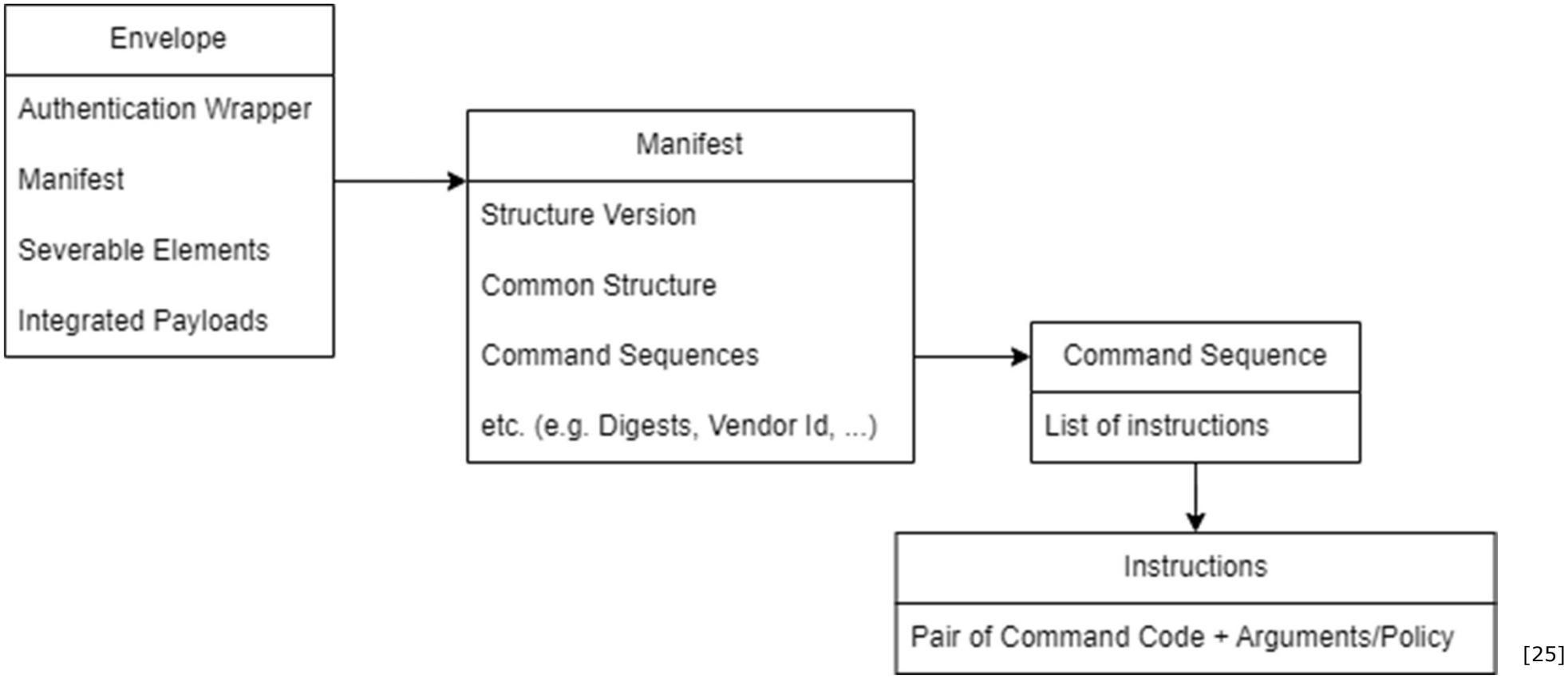
FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# SUIT Manifest

- ***Overview***
  - RFC9124
    - Manifest Information Model
  - SUIT Manifest
    - Draft version 27
    - CBOR-based
  - Devices require parser

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# SUIT Manifest - Structure




[25]

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# SUIT Manifest

- ***SUIT*** – Command Sequences
  - Common Sequence
    - Set common metadata values
    - Compatibility checks
  - Update Commands
    - Payload Fetch
    - Payload Installation
  - Invocation Commands
    - System Validation
    - Image Invocation

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# SUIT Manifest

```
{
    "manifest": {
        "manifest-version": 1,
        "manifest-sequence-number": 1,
        "common": { /* common structure and sequence */ } ,
        "install": [
            {
                "command-id": "directive-set-parameters",
                "command-arg": {
                    "uri": "coap://[2001:db8::1]/encrypted-image.bin"
                },
                "component-id": [
                    "72616d",
                    "30"
                ]
            },
            {}
        ],
        "validate": [{ /* invocation commands */ }]
    }
}
```

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

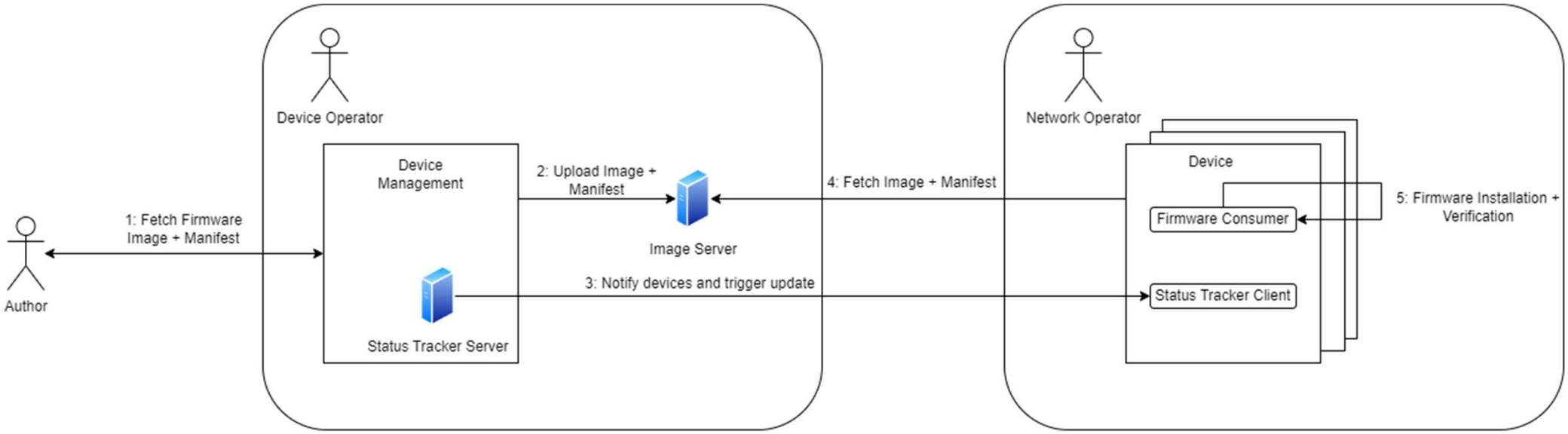
# Firmware Encryption in SUIT

> ***SUIT*** – Firmware Encryption/Decryption

> SUIT example in RIOT
> Mitigate Reverse-Engineering
> draft-ietf-suit-firmware-encryption-20

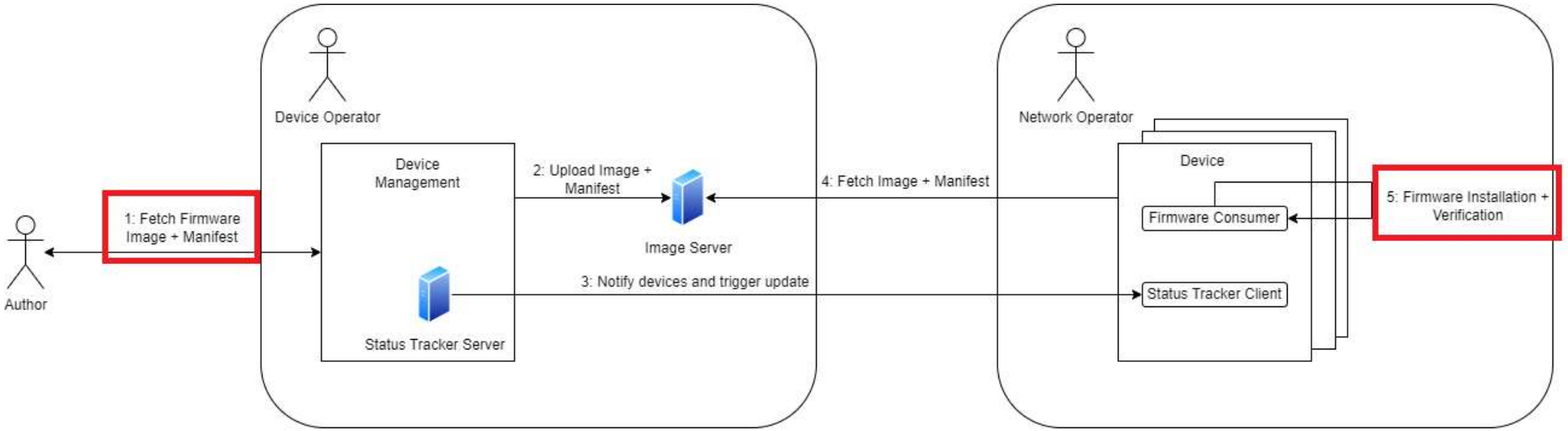
FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Firmware Encryption in SUIT



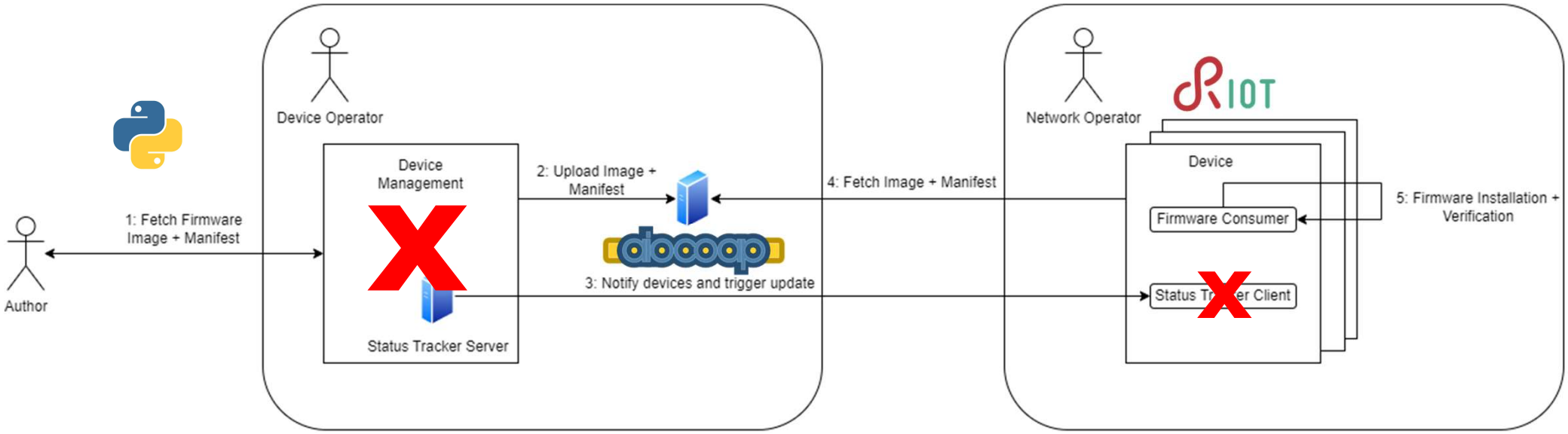
FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Firmware Encryption in SUIT



FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Firmware Encryption in SUIT – Set-Up



FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Firmware Encryption in SUIT

> ***Set-Up*** – Overview
  > Local File Server – ***aiocoap*** [26]
  > Device – ***RIOT Native***
  > Encryption Scheme – ***AES-CCM-128***
    > **Not included: Key Exchange**
  > Verification - ***Wireshark***

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# SUIT Manifest

```
...
{
    "command-id": "directive-override-parameters",
    "command-arg": {
        "nonce": "ad374b7a28f3cc4b56dde2",
        "aad": "504c41494e2d544558542d414144",
        "mac_len": 16,
        "enc_len": 4
    },
    "component-id": [
        "72616d",
        "30"
    ]
},
{
    "command-id": "directive-decrypt-image",
    "command-arg": 15,
    "component-id": [
      "72616d",
      "30"
    ]
}
...
```

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Firmware Update Frameworks

> ***SUIT*** – SW Updates in the IoT

> Let's take a look at an example: SUIT update with RIOT-OS – the friendly OS for the IoT
> https://github.com/RIOT-OS/RIOT/tree/master/examples/suit_update

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

# Reflection

- ***Standardisation effort***
- ***Modular and flexible approach***
- ***Future Work***
  - Physical Devices
  - Key Exchange
  - Update SUIT code base

# Thank you for your attention!
# Secure Firmware Update OTA

Vienna 2024

Miguel Arcilla, Silvie Schmidt

# Sources


(1) K. Zandberg, K. Schleiser, F. Acosta, H. Tschofenig and E. Baccelli, "Secure Firmware Updates for Constrained IoT Devices Using Open Standards: A Reality Check," in IEEE Access, vol. 7, pp. 71907-71920, 2019.

(2) K. Doddapaneni, R. Lakkundi, S. Rao, S. G. Kulkarni and B. Bhat, "Secure FoTA Object for IoT," 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 2017, pp. 154-159.

(3) Atmel Application Note AT02333: http://ww1.microchip.com/downloads/en/AppNotes/Atmel-42141-SAM-AT02333-Safe-and-Secure-Bootloader-Implementation-for-SAM3-4_Application-Note.pdf

(4) Chris Simmonds, OpenIoT Summit 2016: https://elinux.org/images/f/f5/Embedded_Systems_Software_Update_for_IoT.pdf

(5) E. Ronen, A. Shamir, A. Weingarten and C. O'Flynn, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction," 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2017, pp. 195-212.

(6) MCUboot Project, https://mcuboot.com/

(7) TUF – The Update Framework, https://theupdateframework.io/

(8) Zhu, Xiaorui & Tao, Xianping & Gu, Tao & Lu, Jian. (2016). ReLog: A systematic approach for supporting efficient reprogramming in wireless sensor networks. Journal of Parallel and Distributed Computing. 102. 10.1016/j.jpdc.2016.12.010.

(9) Levis, Philip & Culler, David. (2002). Mate: A Tiny Virtual Machine for Sensor Networks. ACM SIGARCH Computer Architecture News. 30. 10.1145/605397.605407.

(10) Kuppusamy, Trishank & DeLong, Lois & Cappos, Justin. (2018). Uptane: Security and Customizability of Software Updates for Vehicles. IEEE Vehicular Technology Magazine. PP. 1-1. 10.1109/MVT.2017.2778751.

(11) Uptane Project, https://uptane.github.io/

(12) Uptane Design, https://uptane.github.io/design.html


Accessed on Nov.21st,21.

# Sources


(13) IETF-SUIT, https://tools.ietf.org/html/draft-ietf-suit-architecture-08

(14) Nikitin, Kirill & Kokoris-Kogias, Eleftherios & Jovanovic, Philipp & Gasser, Linus & Gailly, Nicolas & Khoffi, Ismail & Cappos, Justin & Ford, Bryan. (2018). CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds.

(15) SWUpdate Project, https://sbabic.github.io/swupdate/swupdate.html

(16) LWM2M – Lightweigth M2M, https://www.omaspecworks.org/what-is-oma-specworks/iot/lightweight-m2m-lwm2m/

(17) CoMI – CoAP Management Interface, https://tools.ietf.org/html/draft-ietf-core-comi-04

(18) OCF – Open Connectivity Foundation, https://openconnectivity.org/

(19) TR69 Protocol, https://www.broadband-forum.org/download/TR-069_Amendment-2.pdf

(20) RIOT-OS, https://www.riot-os.org/

(21) https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf

(22) Missbach, N., Secure Firmware Updates for the Internet of ThingsThe IoT, Over-The-Air Updates and possible Solutions, http://pub.fh-campuswien.ac.at/obvfcwhsacc/content/titleinfo/3431921

(23) http://clipart-library.com/

(24) https://www.st.com/resource/en/application_note/dm00355688-overview-secure-firmware-install-sfi-stmicroelectronics.pdf

(25) https://datatracker.ietf.org/doc/html/draft-ietf-suit-manifest-25

(26) https://github.com/chrysn/aiocoap