Hackathon on Lightweight IoT Security Project Pitches

Paris, France | 21-22 May 2024

parishackathon.lakewg.org

Inria OpenSwarm

Crypto agility in lakers

- lakers is an implementation of EDHOC (RFC 9528) in Rust
  - https://github.com/openwsn-berkeley/lakers
- right now, it supports:
  - Cipher Suite 2 (AES-CCM-16-64-128, SHA-256, 8, P-256, ES256, AES-CCM-16-64-128, SHA-256)
  - Authentication mode Static-Static
- the plan is to add support for more cipher suites and authentication methods

Project champion

- Geovane Fedrecheski

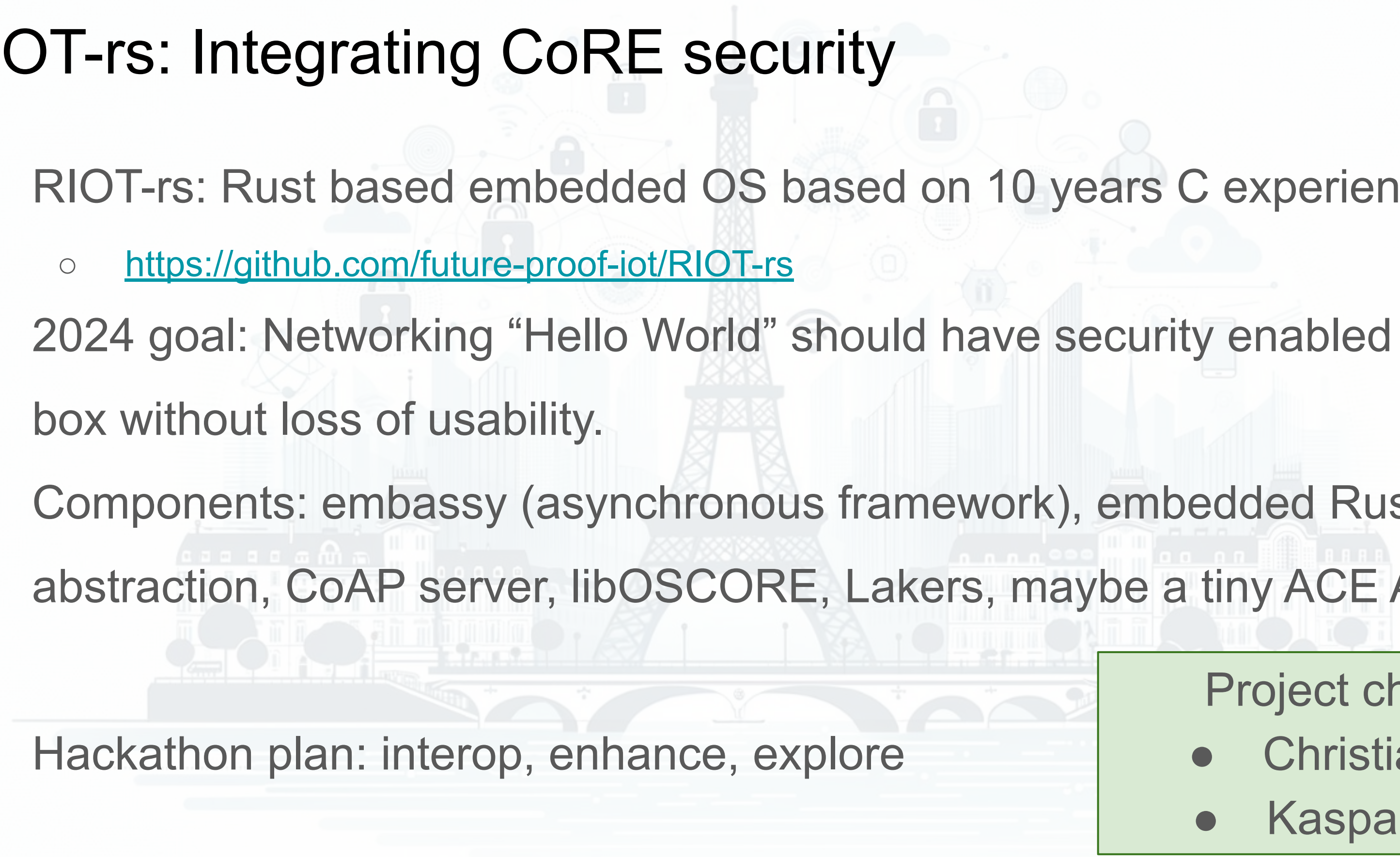
Porting lakers to Single-Chip µicro Motes (SCµM)

- lakers: implementation of EDHOC dedicated for resource-constrained devices
  - https://github.com/openwsn-berkeley/lakers
- SCuM: crystal-free, 2x3 mm2 single-die solution for wireless sensor networks
  - integrating sensing, computation and communication capabilities
  - 802.15.4 compatible transceiver
  - https://github.com/PisterLab/scum-test-code
- Hackathon plan: exploring the feasibility of executing an authenticated key exchange between SCµM and nRF52840-DK

Project champion

- Sara Faour

RIOT-rs: Integrating CoRE security

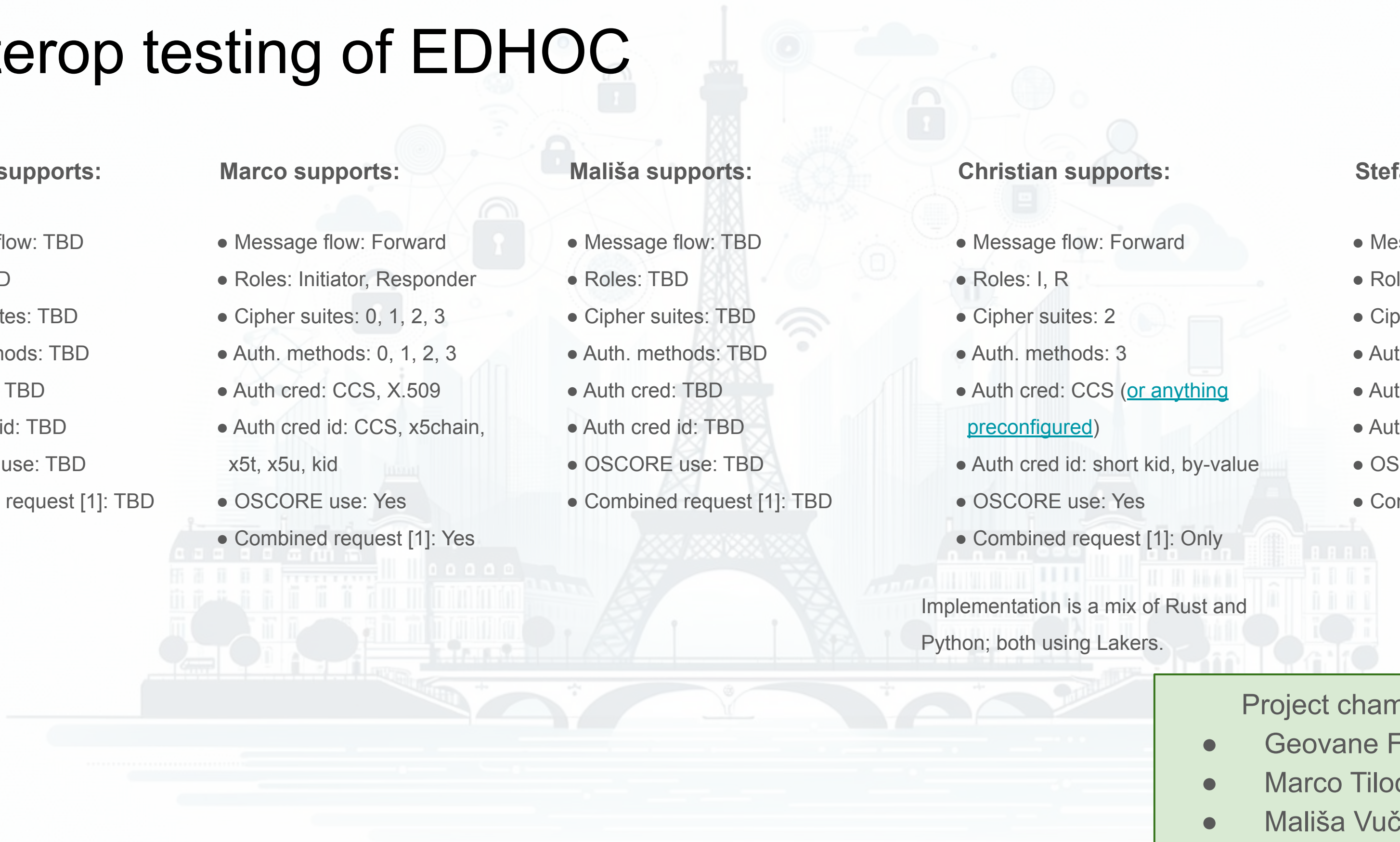


- RIOT-rs: Rust based embedded OS based on 10 years C experience in RIOT
  - https://github.com/future-proof-iot/RIOT-rs
- 2024 goal: Networking “Hello World” should have security enabled out of the box without loss of usability.
- Components: embassy (asynchronous framework), embedded Rust network abstraction, CoAP server, libOSCORE, Lakers, maybe a tiny ACE AS
- Hackathon plan: interop, enhance, explore

Project champions

- Christian Amsüss
- Kaspar Schleiser

Interop testing of EDHOC



Geovane supports:

- Message flow: TBD
- Roles: TBD
- Cipher suites: TBD
- Auth. methods: TBD
- Auth cred: TBD
- Auth cred id: TBD
- OSCORE use: TBD
- Combined request [1]: TBD

Marco supports:

- Message flow: Forward
- Roles: Initiator, Responder
- Cipher suites: 0, 1, 2, 3
- Auth. methods: 0, 1, 2, 3
- Auth cred: CCS, X.509
- Auth cred id: CCS, x5chain, x5t, x5u, kid
- OSCORE use: Yes
- Combined request [1]: Yes

Mališa supports:

- Message flow: TBD
- Roles: TBD
- Cipher suites: TBD
- Auth. methods: TBD
- Auth cred: TBD
- Auth cred id: TBD
- OSCORE use: TBD
- Combined request [1]: TBD

Christian supports:

- Message flow: Forward
- Roles: I, R
- Cipher suites: 2
- Auth. methods: 3
- Auth cred: CCS (or anything preconfigured)
- Auth cred id: short kid, by-value
- OSCORE use: Yes
- Combined request [1]: Only

Implementation is a mix of Rust and Python; both using Lakers.

Stefan supports:

- Message flow: TBD
- Roles: TBD
- Cipher suites: TBD
- Auth. methods: TBD
- Auth cred: TBD
- Auth cred id: TBD
- OSCORE use: TBD
- Combined request [1]: TBD

Project champions

- Geovane Fedrecheski
- Marco Tiloca
- Mališa Vučinić
- Christian Amsüss
- Stefan Hristozov

[1] https://datatracker.ietf.org/doc/draft-ietf-core-oscore-edhoc/

EDHOC and OSCORE profile of the ACE framework

- Building on Eclipse Californium, with CoAP (RFC 7252) and OSCORE (RFC 8613) …
- Implementation of ACE-OAuth Framework (RFC 9200) and its OSCORE profile (RFC 9203)
  - https://bitbucket.org/marco-tiloca-sics/ace-java/src/master/
- Implementation of the authenticated key establishment protocol EDHOC (RFC 9528)
  - https://github.com/rikard-sics/californium/tree/edhoc
- Goal: implement the EDHOC and OSCORE profile of ACE
  - https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/
  - Development branch: https://bitbucket.org/marco-tiloca-sics/ace-java/src/edhoc-oscore-profile/
  - Starting from a setup with the OSCORE profile:
    - Set a node to be both ACE Client and EDHOC Initiator
    - Set a node to be both ACE Resource Server and EDHOC Responder
    - Morph the OSCORE profile into the EDHOC and OSCORE profile

Project champion:
Marco Tiloca

Interop testing of EAP-EDHOC

Project champions

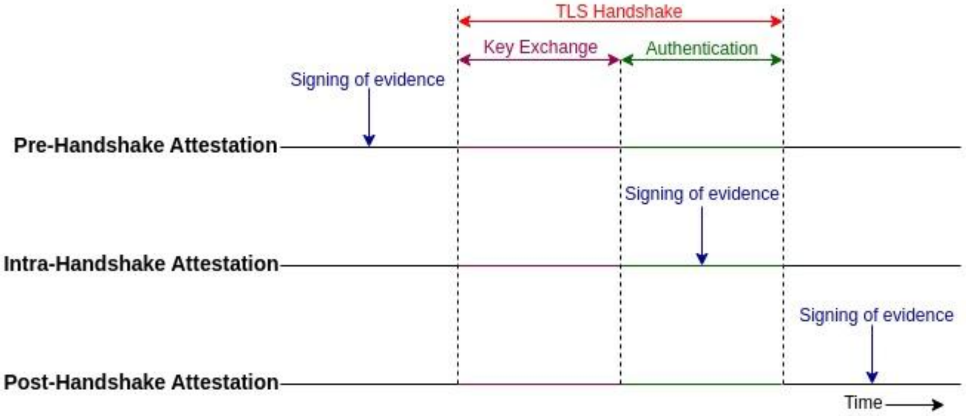
- Rafa Marin-Lopez
- Dan Garcia-Carrillo

- Developing & Testing EAP-EDHOC implementations
  - UM and UNIOVI's (so far)
- Need for an agreement in a common EDHOC implementation (or interoperable)
  - uoscore-uedhoc implementation (UM's version 3.0.2)
- UM implementation
  - EAP peer: wpa_supplicant 2.10 or 2.11-dev (also supports EAP-TLS (v1.3))
  - EAP authenticator: hostapd 2.10 or 2.11-dev
  - EAP server: Freeradius 3.2.3
- UNIOVI implementation
  - EAP peer and authenticator: OpenPANA 0.2.4
  - EAP server: FreeRADIUS 3.2.1
- Interop plan:
  - UM EAP peer and authenticator (wpa_supplicant/hostapd) and UNIOVI's EAP server (FreeRADIUS)
  - UNIOVI's EAP peer and authenticator (OpenPANA) and UM's EAP server (FreeRADIUS)

Formal Verification of Attested TLS

- 3 main ways to combine attestation in TLS (Background-check model)

1. Pre-handshake attestation (Overview slides)
2. Intra-handshake attestation (IETF draft)
3. Post-handshake attestation (Project proposal)



Background on Attestation

- Formal Specs
- Formal analysis artifacts repo

Hackathon plan

- Make progress on open issues
- Flexible to adapt to interests of participants

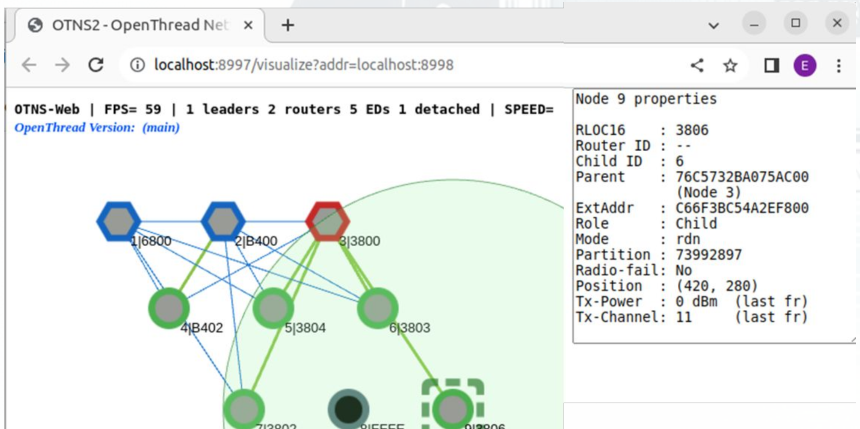
Project champion

- Muhammad Usama Sardar

Constrained BRSKI (cBRSKI) Onboarding for Thread devices

- Preparing for cBRSKI testing in Thread mesh networks: use the simulator!
- Around day 2, virtual Thread nodes should be able to connect with external UDP clients & servers: this simulates apps/protocols on the node.
- Code: release https://github.com/EskoDijk/ot-ns/

  Hackathon branch: https://github.com/EskoDijk/ot-ns/tree/pr-ccm

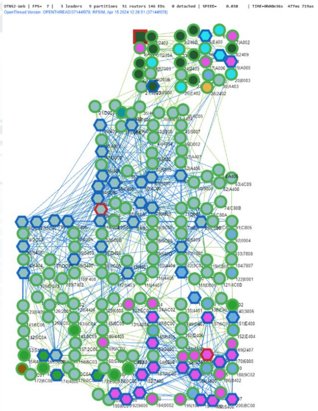


```
OTNS-Web | FPS= 59 | 1 leaders 2 routers 5 EDs 1 detached | SPEED=
```

OpenThread Version: (main)

```
Node 9 properties

RLOC16     : 3806
Router ID  : --
Child ID   : 6
Parent     : 76C5732BA075AC00
             (Node 3)
ExtAddr    : C66F3BC54A2EF800
Role       : Child
Mode       : rdn
Partition  : 73992897
Radio-fail: No
Position   : (420, 280)
Tx-Power   : 0 dBm  (last fr)
Tx-Channel: 11      (last fr)
```



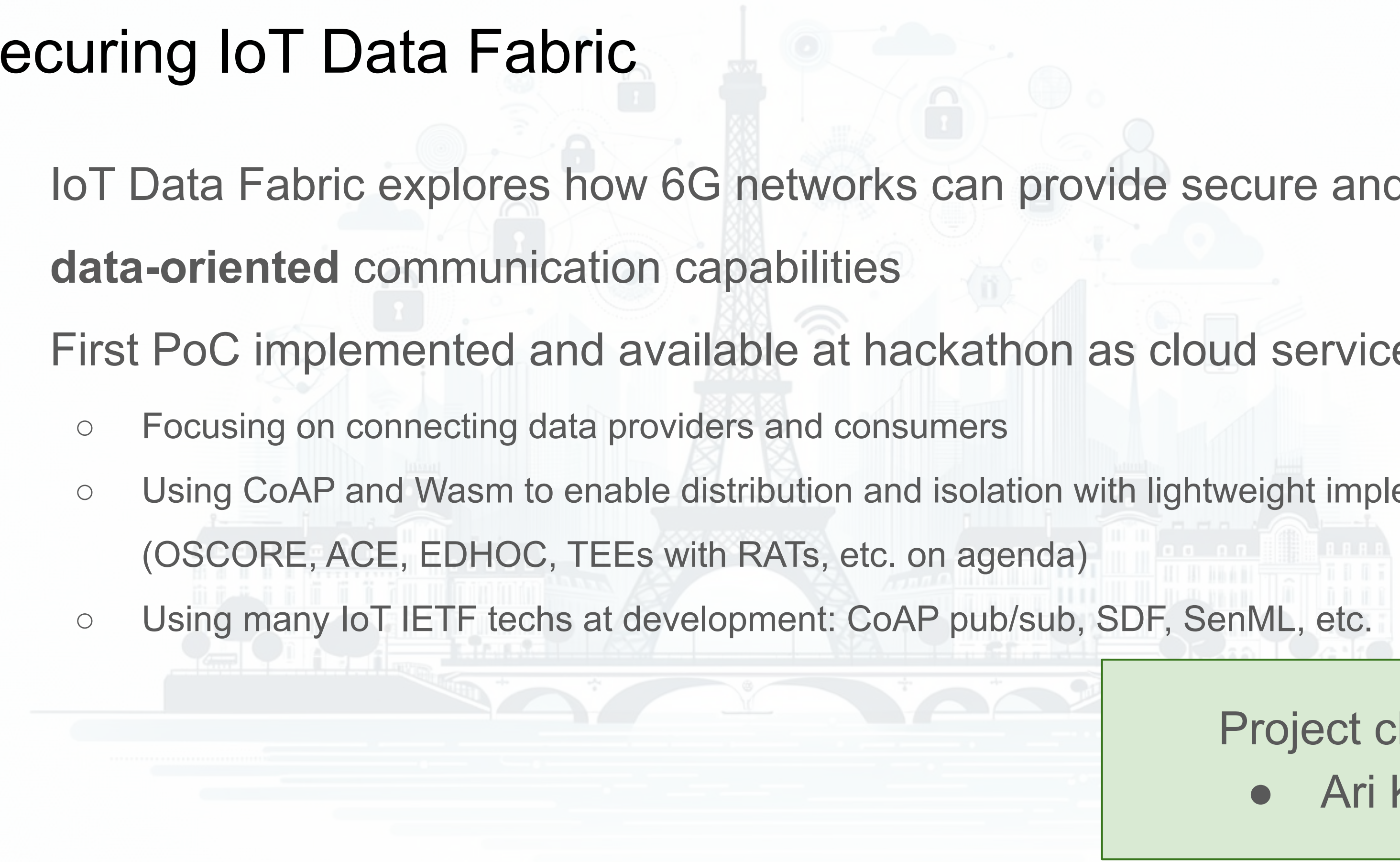
```
OTNS2-Web | FPS=  7 |   3 leaders   9 partitions  51 routers 146 EDs   0 detached | SPEED=    0.038    | TIME=0h00m36s  477ms 719us
```

OpenThread Version: OPENTHREAD/37144f078, RFSIM, Apr 15 2024 12:28:51 (37144f078)

Project champion

- Esko Dijk

Securing IoT Data Fabric



- IoT Data Fabric explores how 6G networks can provide secure and scalable **data-oriented** communication capabilities
- First PoC implemented and available at hackathon as cloud service
  - Focusing on connecting data providers and consumers
  - Using CoAP and Wasm to enable distribution and isolation with lightweight implementations (OSCORE, ACE, EDHOC, TEEs with RATs, etc. on agenda)
  - Using many IoT IETF techs at development: CoAP pub/sub, SDF, SenML, etc.

Project champion

- Ari Keränen

Hackathon on Lightweight IoT Security Side Meetings

Paris, France | 21-22 May 2024

parishackathon.lakewg.org

Inria OpenSwarm

Meeting: T2TRG Interim Meeting

When: Tue 17:00-18:50
Where: Room A115

- IoT security implementation, operation, and systems aspects

17:00	Chairs	Intro
17:10	Rajat Kandoi / Ari Keränen	Secure In-network Data Fabric for IoT applications
17:27	Abhishek Kumar	How can AI be distributed in the computing continuum? Introducing the neural pub/sub paradigm
17:44	Renzo Navas	Post-Quantum Cryptography: Overview and IoT Standardisation Perspectives
18:01	Marco Tiloca	Distribution of Software Updates with End-to-End Secure Group Communication for CoAP
18:18	Rikard Höglund	Using onion routing with CoAP
18:35	Chairs	Wrapup

Meeting: lake-authz and link layer technologies

- one use case of lake-authz is **network join**
- lake-authz will be more useful if it can be used in several link layer technologies
  - some technologies are easier to integrate, some are harder
  - most already provide a join procedure
- guiding questions:
  - how to integrate lake-authz in different link layer technologies?
  - which technologies are easier/harder to integrate?
  - which technologies' join procedure can be improved by lake-authz? and how?
  - is there something in the draft we could do to make it easier?

When: **Wed, 16:15**
Where: Room A115

Meeting: Interactive tutorial: Towards formal verification of attested TLS

- Overview of attestation
  - RATS architecture
- Overview of TLS
- Overview of attested TLS
- Intro to formal verification
- Formal verification of attested TLS
  - RA-TLS in RATS background-check model
- Intention is:
  - To share our “attested TLS” journey to help “attestation over EDHOC” ID make progress by learning the design concepts

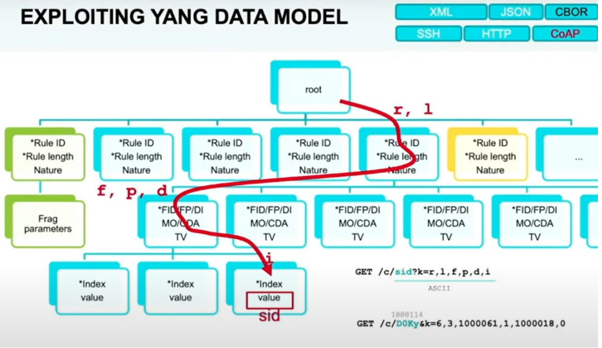
When: Tue, 09:45
Where: Breakout Room

Meeting: Secure Application Performance Management (APM) using CORECONF

When: Tue, 13:30

Where: Room A115

- What state-of-the-art implementations of CORECONF do exist?
  - “CoMI had little use because its specification was still under draft, and no open-source implementations existed at the time. Since Sinche et al.’s survey, CoMI was renamed to CORECONF and its working group have a GitHub project which does not appear to be ready for production use” - A Proposal and Experimental Evaluation Towards Mass Configuration of Heterogeneous IIoT Nodes
  - Use of CORECONF in Static Context Header Compression (SCHC) - YouTube Recording of Future IoT School in Berlin, 2022
  - Python CORECONF Library - pycoreconf - Github Link
- Discussion about how CORECONF can be used in APM
  - Collecting Ideas for Use-Cases
  - Implementation hints for an implementation in C on a MCU
  - Security Aspects of CORECONF

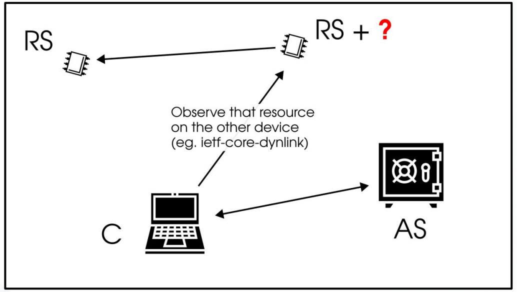


EXPLOITING YANG DATA MODEL

```
GET /c/sid?k=r,l,f,p,d,i
GET /c/DOKy&k=6,3,1000061,1,1000018,0
```

Meeting: Machine-to-machine setup in ACE

or: “Components we are missing for RIOT-rs”


RS
RS + ?
Observe that resource on the other device (eg. ietf-core-dynlink)
C
AS

- In ACE, usually our devices are RS.
- CoAP affords low-cost device to device communication, and sometimes one device takes a client role.
  How is this best expressed in the ACE context?
  Should all our devices enroll as a Client at the AS?
  Can we “just” send them a token to use along with the URI when we configure which action to take?
- Details: https://github.com/future-proof-iot/RIOT-rs/issues/245

When: Tue, 11:15?
Where: Room X

Hackathon on Lightweight IoT Security

Paris, France | 21-22 May 2024

parishackathon.lakewg.org

Inria OpenSwarm