SECCORE

Security for Constrained RESTful Environments

T2TRG, Pre-IETF118 meeting, November 03, 2023

Göran Selander

What happened to this activity?

— Formally, as a dedicated activity, not much …

— But the topics we identified have progressed

Topics 1(3)

— Attacks on CoAP (**was:** draft-mattsson-core-coap-attacks → **now**: draft-ietf-core-coap-attacks)

— Amplification attacks with CoAP (**was:** draft-mattsson-t2trg-amplification-attacks → **now:** draft-irtf-t2trg-amplification-attacks)

— Efficient and secure tunnelling of CoAP in CoAP (**was:** draft-tiloca-core-oscore-capable-proxies → **now:** draft-ietf-core-oscore-capable-proxies)

— Security context transfer for CoAP transport indication (draft-amsuess-core-transport-indication → …)

— Security for non-traditional response forms (draft-bormann-core-responses → …)

Topics 2(3)

— Key limits and key update for OSCORE (**was:** draft-ietf-core-oscore-key-update →
now: draft-ietf-core-oscore-key-update + draft-ietf-core-oscore-key-limits)

— Firmware update using CoAP group communication (SUIT/CoRE) → storyline and
sketches by Marco, potential side meeting at IETF 118)

— Survey of CoAP group communication security life cycle (CoRE/ACE)

— Pub-sub for CoAP (draft-ietf-core-coap-pubsub, draft-ietf-ace-pubsub-profile
now: active progress in CoRE & ACE)

— Actors in a symmetric authorization architecture (draft-ietf-ace-actors → related
discussion about in ACE/LAKE about power of attorney vs enrolling "Client" and
"Resource Server" roles)

Topics 3(3)

— Authorization to wake device over radio using CoAP (draft-bormann-t2trg-sworn → ...)

— Trustworthy things (https://doi.org/10.1145/3488661.3494034)

  — IoT device able to produce trustworthy evidence about itself using Remote Attestation Procedures

  — a new "trustworthiness" quality that allows to securely bind any information that the device exchanges with a set of trust metrics representing a snapshot of its most recent security state

Other topics?

— ...

What next?

— Is this the right mode of operation?

 — Brainstorm new topics

 — Keep track

 — Present status