SECCORE

Security for Constrained RESTful Environments

New topic series for T2TRG

T2TRG, Pre-IETF113 meeting, March 10, 2022

Göran Selander

Security for CoAP applications

Examples of previous work:

1. Security enhancements of CoAP: Echo, Request-Tag, and Token Processing, RFC 9175 (Feb. 2022)

Done in CoRE WG

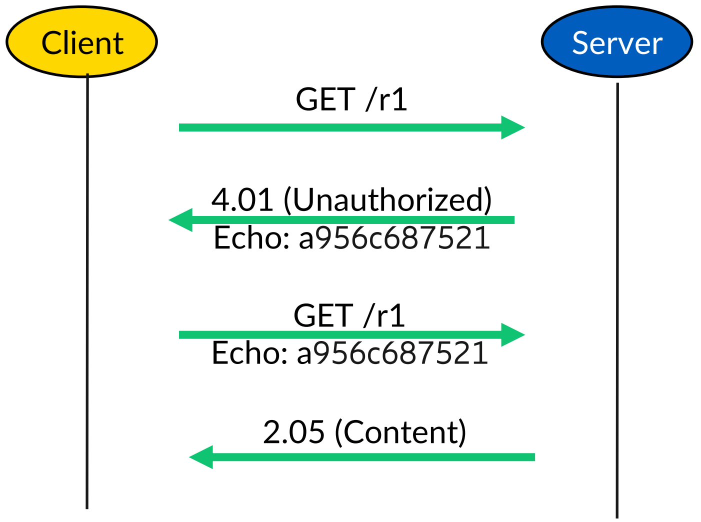
2. Thormarker, E. "On using the same key pair for Ed25519 and an X25519 based KEM" (April 2021)

   - https://eprint.iacr.org/2021/509

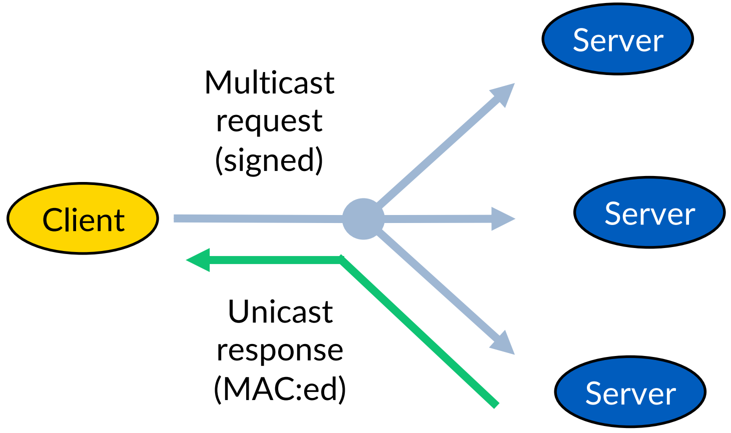
- Verify signature of group message with **CoAP client public key**.
- Derive shared secret using **the same CoAP client public key** and generate MAC for unicast response

Needed by CoRE WG

Ex 1a. Anti-spoofing,, Freshness



Ex 2. Efficient group communication with simplified key management



Rationale for T2TRG/SECCORE

- More work needed on security for CoAP-based applications
- Topics not necessarily in scope of (a single) IETF WG
- Matching the T2TRG charter [1]
- Provide a space allowing regular attendance
  - Gather researchers and others who are interested
- Recurring meetings
  - Progress research
  - Explain topics
- Report at T2TRG summary meetings

[1] https://datatracker.ietf.org/doc/charter-irtf-t2trg/

Excerpts from T2TRG charter:

- *"issues that touch opportunities for standardization in the IETF"*
- *"low-resource nodes ("things", "constrained nodes") can communicate among themselves and with the wider Internet"*
- *"Deployment considerations; scaling considerations; cost of ownership "*
- *"Lifecycle aspects (including, but not limited to, security considerations)*
- *"Operating "things" that have multiple masters/stakeholders*
- *"Exploring the duality of state- and event-based approaches"*

Types of work in SECCORE

- Specific research topics
  - Like example 2 in slide 2
- Survey-based improvements of state of the art
  - Like RFC 8576 ”IoT Security: State of the Art and Challenges”
- Topics spanning multiple IETF WGs (such as CoRE, ACE, LAKE , SUIT, COSE, RATS, ANIMA, etc.) without an established home
  - Like the example in the next slide (*)

The result is expected to be useful in the context of IETF standards.

Topics for inspiration

- Attacks on CoAP (draft-mattsson-core-coap-attacks)
- **Amplification attacks with CoAP (draft-mattsson-t2trg-amplification-attacks)**
- Efficient and secure tunnelling of CoAP in CoAP (draft-tiloca-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)
- Key limits and key update for OSCORE (draft-ietf-core-oscore-key-update)
- **Firmware update using CoAP group communication (SUIT/CoRE)***
- Survey of CoAP group communication security life cycle (CoRE/ACE)
- Pub-sub for CoAP (draft-ietf-core-coap-pubsub, draft-ietf-ace-pubsub-profile)
- Actors in a symmetric authorization architecture (draft-ietf-ace-actors)
- Authorization to wake device over radio using CoAP (draft-bormann-t2trg-sworn)
- Trustworthy things (https://doi.org/10.1145/3488661.3494034)

Misc.

- Grouping topics into short- / mid- / long-term

- Identifying “penholders” that prepare a topic for SECCORE
  - By providing starting points (where relevant) for:
    - use cases (where helpful below)
    - problem statement (and why is this relevant to T2TRG/SECCORE),
    - available components / missing components,
    - recent new opportunities,
    - success factors, e.g. defining criteria for efficiency,
    - areas that require different solution sets,
    - threat models,
    - actor models,
    - …

Discussion

— Do we need more planning or should we just try it out?

— First topic follow suite: Amplification attacks
— Candidate second topic: Firmware update using multicast
— Proposals for topics/penholders are welcome!

— Other comments?