Applying Generate Random Extensions And Sustain Extensibility (GREASE) to EDHOC Extensibility

draft-amsuess-core-edhoc-grease

Christian Amsüss

IETF118 Prague, LAKE, 2023-11-06

Long time ago in London...

"EDHOC will start small and then add all things in TLS back in."

Let's be selective – and then mindfully take good parts (e. g. RFC 8701).

GREASE

- EDHOC has extension points
- Implementations often just see what they expect
- Middleboxes can often just deal with what they expect

...so if extension points go unused, they might become unusable.

We apply GREASE to prevent the joins from rusting shut.

Concrete extension points

- ✔ EAD items: 1× 1+1, 3× 1+2; all optional
- ✔ Cipher suites: 1× 1+1, 3× 1+2; responder can't select them
- ? Methods: Not negotiated
- ? COSE headers: Not negotiated

...and if we could do the latter, should we?

Caveats

- We're message size constrained.
  → Apply it in applications where the added size will be tolerable.
- It can be a covert channel (cf. INTDIR on padding).
  → Yes. As can the use of any other EAD.
- The distribution and values of options reveal some data about the implementation.
  → Concrete recommendation available on size and choice – large anonymity set.

Advancing GREASE for EDHOC

- Check against RFC 9170 guidance.
- Check against draft edm-protocol-greasing and upcoming work.
- Fit in the WG?
- Should be an easy document.