Security Dispatch WG
(SecDispatch)

Tuesday, March 5, 2019

Virtual Interim Meeting

Richard Barnes and Roman Danyliw

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.
As a reminder:
By participating in the IETF, you agree to follow IETF processes and policies.

If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.

As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.

Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

Dispatch Process

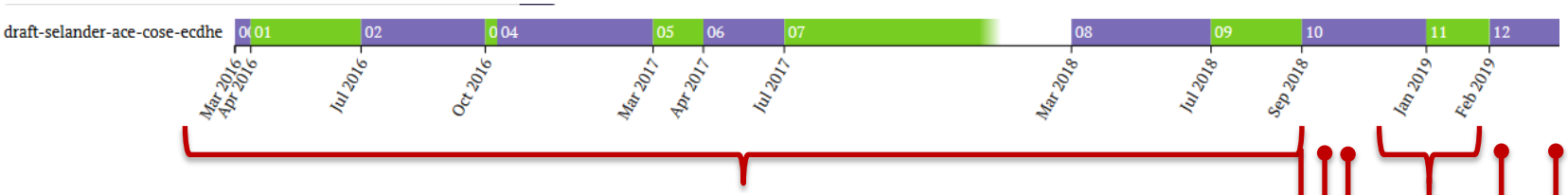
Ground Rules

- SecDispatch recommends next steps for new work
- SecDispatch DOES NOT adopt drafts

Possible Outcomes

- Direction to an existing WG
- Propose a new, focused WG
- AD-sponsorship (assuming AD is willing)
- IETF should not work on this topic

EDHOC Timeline



Motivated by ACE WG

IETF 103 (2018-11-06)
Defer ACE WG Call for Adoption in favor of SecDispatch

Formal Verification on -08 (2018-11-26)
Bruni, A. Jørgensen, T. Petersen, T. Schürmann, C. *Formal Verification of Ephemeral Diffie-Hellman Over COSE (EDHOC).* SSR 2018 : Security Standardisation Research. November 26, 2018.

Robust Mailing List Conversation (2018-12 to 2019-02)
See: ACE and SECDISPATCH LIST

CRFG Review on -12 (2019-02-26)
https://mailarchive.ietf.org/arch/msg/cfrg/6WN2C2RYGTIAInE2jIUco6L9pO8

SecDispatch Virtual Interim (2019-03-05)

Agenda

(1) Opening (chairs, 5 min)
- SecDispatch Process Overview
- Framing the EDHOC Discussion -- draft-selander-ace-cose-ecdhe

(2) Problem Statement (15 min)
- Motivating use case(s) for EDHOC (Goran Selander)
- Requirements of EDHOC use cases (Goran Selander)

(3) EDHOC as a Solution (15 min)
- EDHOC security and non-security objectives (Goran Selander)
- Protocol design (Goran Selander)

(4) Analysis of Alternatives (Goran Selander + Jim Schaad, 20 min)
- Benchmarking current solutions and EDHOC

(5) Formal Verification of EDHOC (Alessanro Bruni, 20 min)

(6) Open Mic and Next Steps (all, 20 min)