IP Security Maintenance and Extensions (IPsecME) WG

IETF 119, Tuesday, March 19th, 2024

Chairs: Tero Kivinen
Yoav Nir

Responsible AD: 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)

Administrative Tasks

We need volunteers to be:

- Two note takers

MeetEcho: https://meetings.conf.meetecho.com/ietf119/?session=32044

Notes: https://notes.ietf.org/notes-ietf-119-ipsecme

Agenda

- Note Well, technical difficulties and agenda bashing – Chairs (5 min) (15:30-15:35)
- Document Status – Chairs (5 min) (15:35-15:40)
- Presentations
  - Post-quantum Hybrid Key Exchange with ML-KEM in the IKEv2 – Scott Fluhrer (5 min) (15:40-15:45)
  - ESP Echo Protocol – Jen Linkova (15 min) (15:45-16:00)
  - Shared Use of IPsec Tunnel in a Multi-VPN Environment – Wei Pan (10 min) (16:00-16:10)
  - IKEv2 Support for Anti-Replay Status Notification – Wei Pan (10 min) (16:10-16:20)
  - Using ShangMi in the IKEv2 – Frank (Liang) XIA (10 min) (16:20-16:30)
  - IKEv2 IPv4 Downstream Fragmentation – Daniel Migault (10 min) (16:30-16:40)
  - IKEv2 DSCP Notification – Daniel Migault (10 min) (16:40-16:50)
- AOB + Open Mic (10 min) (16:50-17:00)

WG Status Report

- Published as RFCs
  - Internet Key Exchange Protocol Version 2 (IKEv2) Configuration for Encrypted DNS RFC9464
- IETF Last Call:
  - draft-ietf-ipsecme-ikev2-auth-announce
- Almost Publication Requested (waiting for document update):
  - draft-ietf-ipsecme-multi-sa-performance

WG Status Report

- Waiting for write-up / AD Followup:
  - draft-ietf-ipsecme-g-ikev2
- Work in progress:
  - draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt
  - draft-smyslov-ipsecme-ikev2-qr-alt
  - draft-mglt-ipsecme-ikev2-diet-esp-extension
  - draft-mglt-ipsecme-diet-esp
- Expired:
  - draft-ietf-ipsecme-ike-tcp

Presentations

- Post-quantum Hybrid Key Exchange with ML-KEM in the IKEv2
  Scott Fluhrer
- ESP Echo Protocol
  Jen Linkova
- Shared Use of IPsec Tunnel in a Multi-VPN Environment
  Wei Pan
- IKEv2 Support for Anti-Replay Status Notification
  Wei Pan
- Using ShangMi in the IKEv2
  Frank (Liang) XIA
- IKEv2 IPv4 Downstream Fragmentaton
  Daniel Migault
- IKEv2 DSCP Notification
  Daniel Migault

Presentations

- **Post-quantum Hybrid Key Exchange with ML-KEM in the IKEv2**
  Scott Fluhrer
- ESP Echo Protocol
  Jen Linkova
- Shared Use of IPsec Tunnel in a Multi-VPN Environment
  Wei Pan
- IKEv2 Support for Anti-Replay Status Notification
  Wei Pan
- Using ShangMi in the IKEv2
  Frank (Liang) XIA
- IKEv2 IPv4 Downstream Fragmentaton
  Daniel Migault
- IKEv2 DSCP Notification
  Daniel Migault

Presentations

- Post-quantum Hybrid Key Exchange with ML-KEM in the IKEv2
  Scott Fluhrer
- **ESP Echo Protocol**
  Jen Linkova
- Shared Use of IPsec Tunnel in a Multi-VPN Environment
  Wei Pan
- IKEv2 Support for Anti-Replay Status Notification
  Wei Pan
- Using ShangMi in the IKEv2
  Frank (Liang) XIA
- IKEv2 IPv4 Downstream Fragmentaton
  Daniel Migault
- IKEv2 DSCP Notification
  Daniel Migault

Presentations

- Post-quantum Hybrid Key Exchange with ML-KEM in the IKEv2
  Scott Fluhrer
- ESP Echo Protocol
  Jen Linkova
- **Shared Use of IPsec Tunnel in a Multi-VPN Environment**
  Wei Pan
- IKEv2 Support for Anti-Replay Status Notification
  Wei Pan
- Using ShangMi in the IKEv2
  Frank (Liang) XIA
- IKEv2 IPv4 Downstream Fragmentaton
  Daniel Migault
- IKEv2 DSCP Notification
  Daniel Migault

Presentations

- Post-quantum Hybrid Key Exchange with ML-KEM in the IKEv2
  Scott Fluhrer
- ESP Echo Protocol
  Jen Linkova
- Shared Use of IPsec Tunnel in a Multi-VPN Environment
  Wei Pan
- **IKEv2 Support for Anti-Replay Status Notification**
  Wei Pan
- Using ShangMi in the IKEv2
  Frank (Liang) XIA
- IKEv2 IPv4 Downstream Fragmentaton
  Daniel Migault
- IKEv2 DSCP Notification
  Daniel Migault

Presentations

- Post-quantum Hybrid Key Exchange with ML-KEM in the IKEv2
  Scott Fluhrer
- ESP Echo Protocol
  Jen Linkova
- Shared Use of IPsec Tunnel in a Multi-VPN Environment
  Wei Pan
- IKEv2 Support for Anti-Replay Status Notification
  Wei Pan
- **Using ShangMi in the IKEv2**
  Frank (Liang) XIA
- IKEv2 IPv4 Downstream Fragmentaton
  Daniel Migault
- IKEv2 DSCP Notification
  Daniel Migault

Presentations

- Post-quantum Hybrid Key Exchange with ML-KEM in the IKEv2
  Scott Fluhrer
- ESP Echo Protocol
  Jen Linkova
- Shared Use of IPsec Tunnel in a Multi-VPN Environment
  Wei Pan
- IKEv2 Support for Anti-Replay Status Notification
  Wei Pan
- Using ShangMi in the IKEv2
  Frank (Liang) XIA
- **IKEv2 IPv4 Downstream Fragmentaton**
  Daniel Migault
- IKEv2 DSCP Notification
  Daniel Migault

Presentations

- Post-quantum Hybrid Key Exchange with ML-KEM in the IKEv2
  Scott Fluhrer
- ESP Echo Protocol
  Jen Linkova
- Shared Use of IPsec Tunnel in a Multi-VPN Environment
  Wei Pan
- IKEv2 Support for Anti-Replay Status Notification
  Wei Pan
- Using ShangMi in the IKEv2
  Frank (Liang) XIA
- IKEv2 IPv4 Downstream Fragmentaton
  Daniel Migault
- **IKEv2 DSCP Notification**
  Daniel Migault

Open Discussion

- Other points of interest?