IP Security Maintenance and Extensions (IPsecME) WG

IETF 120, Tuesday,July 23th, 2024

Chairs: Tero Kivinen
Yoav Nir

Responsible AD: Deb Cooley

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/ietf120/?session=33058

Notes: https://notes.ietf.org/notes-ietf-120-ipsecme

Agenda

- Note Well, technical difficulties and agenda bashing – Chairs (2 min) (15:30-15:32)
- Document Status – Chairs (3 min) (15:32-15:35)
- Presentations
  - Delete info -- Paul Wouters (3 min) (15:35-15:38)
  - SA TS Payloads opt -- Paul Wouters (4 min) (15:38-15:42)
  - Anti replay notification -- Paul Wouters (4 min) (15:42-15:46)
  - Child PFS info -- Paul Wouters (4 min) (15:46-15:50)
  - ESP Echo Protocol -- Jen Linkova (10 min) (15:50-16:00)
  - Encrypted ESP Ping -- Antony Antony (10 min) (16:00-16:10)
  - Beet mode -- Antony Antony (10 min) (16:10-16:20)
  - Multiple sequence counters -- Steffen Klassert (5 min) (16:20-16:25)
  - WESPv2 -- Steffen Klassert (15 min) (16:25-16:40)
  - Diet-ESP -- Daniel Migault (5 min) (16:40-16:45)
  - FrodoKEM in IKEv2 -- Wang Guilin (5 min) (16:45-16:50)
  - PQC Auth -- Valery Smyslov (10 min) (16:50-17:00)
- AOB + Open Mic (0 min) (16:50-17:00)

WG Status Report

- Published as RFCs
  - Internet Key Exchange Protocol Version 2 (IKEv2) Support for Per-Resource Child Security Associations (SAs) RFC9611
  - Announcing Supported Authentication Methods in the IKEv2 RFC9593

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

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

Presentations

Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	**Paul Wouters**
ESP Echo Protocol	Jen Linkova
Encrypted ESP Ping	Antony Antony
Beet mode	Antony Antony
Multiple sequence counters	Steffen Klassert
WESPv2	Steffen Klassert
Diet-ESP	Daniel Migault
FrodoKEM in IKEv2	Wang Guilin
PQC Auth	Valery Smyslov

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• **ESP Echo Protocol**	**Jen Linkova**
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• **Encrypted ESP Ping**	**Antony Antony**
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• **Beet mode**	**Antony Antony**
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• **Multiple sequence counters**	**Steffen Klassert**
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• **WESPv2**	**Steffen Klassert**
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• **Diet-ESP**	**Daniel Migault**
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• **FrodoKEM in IKEv2**	**Wang Guilin**
• PQC Auth	Valery Smyslov

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• **PQC Auth**	**Valery Smyslov**

Open Discussion

- Other points of interest?