IP Security Maintenance and Extensions (IPsecME) WG

IETF 116, Wednesday, March 29th, 2023

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/ietf116/?group=ipsecme&short=&item=1

Notes: https://notes.ietf.org/notes-ietf-116-ipsecme

Agenda

- Note Well, technical difficulties and agenda bashing – Chairs (5 min) (15:30-15:35)
- Document Status – Chairs (5 min) (15:35-15:50)
- Presentations
  - Issues SA TS Payloads opt draft – Paul Wouters (10 min) (15:50-16:00)
  - Alternative Approach for Mixing Preshared Keys in IKEv2 for Post-quantum Security – Valery Smyslov (10 min) (16:00-16:10)
  - Extended IKEv2 Payload Format – Valery Smyslov (20 min) (16:10-16:30)
  - Anti replay subspaces – Mohsin Shaikh (10 min) (16:30-16:40)
  - IKEv2 IPv4 Link Maximum Atomic Packet Notification Extension – Daniel Migault (10 min) (16:40-16:50)
  - Traffic Selector for Internet Key Exchange version 2 to add support Differentiated Services Field Codepoints – Daniel Migault (10 min) (16:50-17:00)
- If time permits
  - Inter-domain source address validation using RPKI and IPsec

WG Status Report

- Published as RFCs
  - TCP Encapsulation of Internet Key Exchange Protocol (IKE) and IPsec Packets was published as RFC9329
  - Aggregation and Fragmentation Mode for Encapsulating Security Payload (ESP) and Its Use for IP Traffic Flow Security (IP-TFS) was published as RFC9347
  - A YANG Data Model for IP Traffic Flow Security was published as RFC9348
  - Definitions of Managed Objects for IP Traffic Flow Security was published as RFC9349
- RFF Editor queue:
  - draft-ietf-ipsecme-ikev1-algo-to-historic
  - draft-ietf-ipsecme-ikev2-multiple-ke
- Publication requested:
  - draft-ietf-ipsecme-labeled-ipsec IETF Last Call

WG Status Report

- Waiting for write-up / AD Followup:
  - draft-ietf-ipsecme-add-ike
- Working Group Last Call:
  - draft-ietf-ipsecme-auth-announce
  - draft-ietf-ipsecme-g-ikev2
- Work in progress:
  - draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt
  - draft-ietf-ipsecme-multi-sa-performance

Presentations

- Issues SA TS Payloads opt draft – Paul Wouters
- Alternative Approach for Mixing Preshared Keys in IKEv2 for Post-quantum Security – Valery Smyslov
- Extended IKEv2 Payload Format – Valery Smyslov
- Anti replay subspaces – Mohsin Shaikh
- IKEv2 IPv4 Link Maximum Atomic Packet Notification Extension – Daniel Migault
- Traffic Selector for Internet Key Exchange version 2 to add support Differentiated Services Field Codepoints – Daniel Migault
- Inter-domain source address validation using RPKI and IPsec

Presentations

- **Issues SA TS Payloads opt draft – Paul Wouters**
- Alternative Approach for Mixing Preshared Keys in IKEv2 for Post-quantum Security – Valery Smyslov
- Extended IKEv2 Payload Format – Valery Smyslov
- Anti replay subspaces – Mohsin Shaikh
- IKEv2 IPv4 Link Maximum Atomic Packet Notification Extension – Daniel Migault
- Traffic Selector for Internet Key Exchange version 2 to add support Differentiated Services Field Codepoints – Daniel Migault
- Inter-domain source address validation using RPKI and IPsec

Presentations

- Issues SA TS Payloads opt draft – Paul Wouters
- **Alternative Approach for Mixing Preshared Keys in IKEv2 for Post-quantum Security – Valery Smyslov**
- Extended IKEv2 Payload Format – Valery Smyslov
- Anti replay subspaces – Mohsin Shaikh
- IKEv2 IPv4 Link Maximum Atomic Packet Notification Extension – Daniel Migault
- Traffic Selector for Internet Key Exchange version 2 to add support Differentiated Services Field Codepoints – Daniel Migault
- Inter-domain source address validation using RPKI and IPsec

Presentations

- Issues SA TS Payloads opt draft – Paul Wouters
- Alternative Approach for Mixing Preshared Keys in IKEv2 for Post-quantum Security – Valery Smyslov
- **Extended IKEv2 Payload Format – Valery Smyslov**
- Anti replay subspaces – Mohsin Shaikh
- IKEv2 IPv4 Link Maximum Atomic Packet Notification Extension – Daniel Migault
- Traffic Selector for Internet Key Exchange version 2 to add support Differentiated Services Field Codepoints – Daniel Migault
- Inter-domain source address validation using RPKI and IPsec

Presentations

- Issues SA TS Payloads opt draft – Paul Wouters
- Alternative Approach for Mixing Preshared Keys in IKEv2 for Post-quantum Security – Valery Smyslov
- Extended IKEv2 Payload Format – Valery Smyslov
- **Anti replay subspaces – Mohsin Shaikh**
- IKEv2 IPv4 Link Maximum Atomic Packet Notification Extension – Daniel Migault
- Traffic Selector for Internet Key Exchange version 2 to add support Differentiated Services Field Codepoints – Daniel Migault
- Inter-domain source address validation using RPKI and IPsec

Presentations

- Issues SA TS Payloads opt draft – Paul Wouters
- Alternative Approach for Mixing Preshared Keys in IKEv2 for Post-quantum Security – Valery Smyslov
- Extended IKEv2 Payload Format – Valery Smyslov
- Anti replay subspaces – Mohsin Shaikh
- **IKEv2 IPv4 Link Maximum Atomic Packet Notification Extension – Daniel Migault**
- Traffic Selector for Internet Key Exchange version 2 to add support Differentiated Services Field Codepoints – Daniel Migault
- Inter-domain source address validation using RPKI and IPsec

Presentations

- Issues SA TS Payloads opt draft – Paul Wouters
- Alternative Approach for Mixing Preshared Keys in IKEv2 for Post-quantum Security – Valery Smyslov
- Extended IKEv2 Payload Format – Valery Smyslov
- Anti replay subspaces – Mohsin Shaikh
- IKEv2 IPv4 Link Maximum Atomic Packet Notification Extension – Daniel Migault
- **Traffic Selector for Internet Key Exchange version 2 to add support Differentiated Services Field Codepoints – Daniel Migault**
- Inter-domain source address validation using RPKI and IPsec

Presentations

- Issues SA TS Payloads opt draft – Paul Wouters
- Alternative Approach for Mixing Preshared Keys in IKEv2 for Post-quantum Security – Valery Smyslov
- Extended IKEv2 Payload Format – Valery Smyslov
- Anti replay subspaces – Mohsin Shaikh
- IKEv2 IPv4 Link Maximum Atomic Packet Notification Extension – Daniel Migault
- Traffic Selector for Internet Key Exchange version 2 to add support Differentiated Services Field Codepoints – Daniel Migault
- **Inter-domain source address validation using RPKI and IPsec**

Open Discussion

- Other points of interest?