IP Security Maintenance and Extensions (IPsecME) WG

IETF 117, Wednesday, July 28th, 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/ietf117/?group=ipsecme&short=&item=1

Notes: https://notes.ietf.org/notes-ietf-117-ipsecme

Agenda

- Note Well, technical difficulties and agenda bashing – Chairs (5 min) (15:30-15:35)
- Document Status – Chairs (10 min) (15:35-15:45)
- Presentations
  - IKEv2 Optional SA&TS Payloads in Child Exchange – Paul Wouters (15 min) (15:45-16:00)
  - An RPKI and IPsec-based AS-to-AS Approach for Source Address Validation – Ben Schwartz (10 min) (16:00-16:10)
  - Traffic Selector for IKEv2 to add support DSCP – Daniel Migault (5 min) (16:10-16:15)
  - IKEv2 Link Maximum Atomic Packet and Packet Too Big Notification Extension – Daniel Migault (5 min) (16:15-16:20)
  - Diet ESP: ESP Header compression, IKEv2 EHC – Daniel Migault (5 min) (16:20-16:25)
  - Anti-replay sequence number subspaces for traffic-engineered paths and multi-core processing – Mohsin Shaikh (10 min) (16:25-16:35)
  - Use of Reliable Transport in the IKEv2 – Valery Smyslov (10 min) (16:35-16:45)
  - Problem statements and uses cases for lightweight Child Security Associations – Steffen Klassert (10 min) (16:45-16:55)
- Adoption calls – Chairs (5 min) (16:55-17:00)
- AOB + Open Mic (0 min)

WG Status Report

- Published as RFCs
  - Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2) RFC9370
  - Deprecation of the Internet Key Exchange Version 1 (IKEv1) Protocol and Obsoleted Algorithms RFC9395
- RFF Editor queue:
  - draft-ietf-ipsecme-labeled-ipsec
  - draft-ietf-ipsecme-add-ike
- Publication requested:
  - Currently none

WG Status Report

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

Presentations

- IKEv2 Optional SA&TS Payloads in Child Exchange –
  Paul Wouters
- An RPKI and IPsec-based AS-to-AS Approach for Source Address Validation –
  Ben Schwartz
- Traffic Selector for IKEv2 to add support DSCP –
  Daniel Migault
- IKEv2 Link Maximum Atomic Packet and Packet Too Big Notification Extension –
  Daniel Migault
- Diet ESP: ESP Header compression, IKEv2 EHC –
  Daniel Migault
- Anti-replay sequence number subspaces for traffic-engineered paths and multi-core processing –
  Mohsin Shaikh
- Use of Reliable Transport in the IKEv2 –
  Valery Smyslov
- Problem statements and uses cases for lightweight Child Security Associations –
  Steffen Klassert

Presentations

- **IKEv2 Optional SA&TS Payloads in Child Exchange – Paul Wouters**
- An RPKI and IPsec-based AS-to-AS Approach for Source Address Validation – Ben Schwartz
- Traffic Selector for IKEv2 to add support DSCP – Daniel Migault
- IKEv2 Link Maximum Atomic Packet and Packet Too Big Notification Extension – Daniel Migault
- Diet ESP: ESP Header compression, IKEv2 EHC – Daniel Migault
- Anti-replay sequence number subspaces for traffic-engineered paths and multi-core processing – Mohsin Shaikh
- Use of Reliable Transport in the IKEv2 – Valery Smyslov
- Problem statements and uses cases for lightweight Child Security Associations – Steffen Klassert

Presentations

- IKEv2 Optional SA&TS Payloads in Child Exchange –
  Paul Wouters
- **An RPKI and IPsec-based AS-to-AS Approach for Source Address Validation – Ben Schwartz**
- Traffic Selector for IKEv2 to add support DSCP –
  Daniel Migault
- IKEv2 Link Maximum Atomic Packet and Packet Too Big Notification Extension –
  Daniel Migault
- Diet ESP: ESP Header compression, IKEv2 EHC –
  Daniel Migault
- Anti-replay sequence number subspaces for traffic-engineered paths and multi-core processing –
  Mohsin Shaikh
- Use of Reliable Transport in the IKEv2 –
  Valery Smyslov
- Problem statements and uses cases for lightweight Child Security Associations –
  Steffen Klassert

Presentations

- IKEv2 Optional SA&TS Payloads in Child Exchange –
  Paul Wouters
- An RPKI and IPsec-based AS-to-AS Approach for Source Address Validation –
  Ben Schwartz
- **Traffic Selector for IKEv2 to add support DSCP –**
  Daniel Migault
- IKEv2 Link Maximum Atomic Packet and Packet Too Big Notification Extension –
  Daniel Migault
- Diet ESP: ESP Header compression, IKEv2 EHC –
  Daniel Migault
- Anti-replay sequence number subspaces for traffic-engineered paths and multi-core processing –
  Mohsin Shaikh
- Use of Reliable Transport in the IKEv2 –
  Valery Smyslov
- Problem statements and uses cases for lightweight Child Security Associations –
  Steffen Klassert

Presentations

- IKEv2 Optional SA&TS Payloads in Child Exchange –
  Paul Wouters
- An RPKI and IPsec-based AS-to-AS Approach for Source Address Validation –
  Ben Schwartz
- Traffic Selector for IKEv2 to add support DSCP –
  Daniel Migault
- **IKEv2 Link Maximum Atomic Packet and Packet Too Big Notification Extension – Daniel Migault**
- Diet ESP: ESP Header compression, IKEv2 EHC –
  Daniel Migault
- Anti-replay sequence number subspaces for traffic-engineered paths and multi-core processing –
  Mohsin Shaikh
- Use of Reliable Transport in the IKEv2 –
  Valery Smyslov
- Problem statements and uses cases for lightweight Child Security Associations –
  Steffen Klassert

Presentations

- IKEv2 Optional SA&TS Payloads in Child Exchange –
  Paul Wouters
- An RPKI and IPsec-based AS-to-AS Approach for Source Address Validation –
  Ben Schwartz
- Traffic Selector for IKEv2 to add support DSCP –
  Daniel Migault
- IKEv2 Link Maximum Atomic Packet and Packet Too Big Notification Extension –
  Daniel Migault
- **Diet ESP: ESP Header compression, IKEv2 EHC –**
  Daniel Migault
- Anti-replay sequence number subspaces for traffic-engineered paths and multi-core processing –
  Mohsin Shaikh
- Use of Reliable Transport in the IKEv2 –
  Valery Smyslov
- Problem statements and uses cases for lightweight Child Security Associations –
  Steffen Klassert

Presentations

- IKEv2 Optional SA&TS Payloads in Child Exchange –
  Paul Wouters
- An RPKI and IPsec-based AS-to-AS Approach for Source Address Validation –
  Ben Schwartz
- Traffic Selector for IKEv2 to add support DSCP –
  Daniel Migault
- IKEv2 Link Maximum Atomic Packet and Packet Too Big Notification Extension –
  Daniel Migault
- Diet ESP: ESP Header compression, IKEv2 EHC –
  Daniel Migault
- **Anti-replay sequence number subspaces for traffic-engineered paths and multi-core processing –**
  Mohsin Shaikh
- Use of Reliable Transport in the IKEv2 –
  Valery Smyslov
- Problem statements and uses cases for lightweight Child Security Associations –
  Steffen Klassert

Presentations

- IKEv2 Optional SA&TS Payloads in Child Exchange –
  Paul Wouters
- An RPKI and IPsec-based AS-to-AS Approach for Source Address Validation –
  Ben Schwartz
- Traffic Selector for IKEv2 to add support DSCP –
  Daniel Migault
- IKEv2 Link Maximum Atomic Packet and Packet Too Big Notification Extension –
  Daniel Migault
- Diet ESP: ESP Header compression, IKEv2 EHC –
  Daniel Migault
- Anti-replay sequence number subspaces for traffic-engineered paths and multi-core processing –
  Mohsin Shaikh
- **Use of Reliable Transport in the IKEv2 –**
  Valery Smyslov
- Problem statements and uses cases for lightweight Child Security Associations –
  Steffen Klassert

Presentations

- IKEv2 Optional SA&TS Payloads in Child Exchange –
  Paul Wouters
- An RPKI and IPsec-based AS-to-AS Approach for Source Address Validation –
  Ben Schwartz
- Traffic Selector for IKEv2 to add support DSCP –
  Daniel Migault
- IKEv2 Link Maximum Atomic Packet and Packet Too Big Notification Extension –
  Daniel Migault
- Diet ESP: ESP Header compression, IKEv2 EHC –
  Daniel Migault
- Anti-replay sequence number subspaces for traffic-engineered paths and multi-core processing –
  Mohsin Shaikh
- Use of Reliable Transport in the IKEv2 –
  Valery Smyslov
- **Problem statements and uses cases for lightweight Child Security Associations – Steffen Klassert**

WG Adoption calls

- draft-mglt-ipsecme-ts-dscp
- draft-liu-ipsecme-ikev2-mtu-dect
- draft-mglt-ipsecme-diet-esp
- draft-mglt-ipsecme-ikev2-diet-esp-extension
- draft-smyslov-ipsecme-ikev2-qr-alt
- draft-smyslov-ipsecme-ikev2-cookie-revised

Open Discussion

- Other points of interest?