IP Security Maintenance and Extensions (IPsecME) WG

IETF 102, Wednesday, July 18, 2018

Chairs: David Waltermire
Tero Kivinen

Responsible AD: Eric Rescorla

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

Bluesheets

We need volunteers to be:

- Two note takers
- One jabber scribe

Jabber: xmpp:ipsecme@jabber.ietf.org?join

MeetEcho: http://www.meetecho.com/ietf102/ipsecme/

Etherpad:

https://etherpad.tools.ietf.org/p/notes-ietf-102-ipsecme

Agenda

- Agenda bashing, Logistics -- Chairs (5 min) (15:20-15:25)
- Rechartering – Chairs (5 min) (15:25-15:30)
- Draft Status -- Chairs, Valery (10 min) (15:30-15:40)
  - Update on QR IKEv2 -- Valery Smyslov - draft-ietf-ipseme-qr-ikev2
- Work / Other items
  - Split-dns (10 min) – Tommy Pauly (15:40-15:50)
    - draft-ietf-ipsecme-split-dns
  - Auxiliary Exchange in the IKEv2 Protocol (15 min) - Valery Smyslov (15:50-16:05)
    - draft-smyslov-ipsecme-ikev2-aux
  - Postquantum Key Exchange to IKE (10 min) – Scott Fluhrer (16:05-16:15)
    - draft-tjhai-ipsecme-hybrid-qske-ikev2
  - Labeled IPsec (10 min) - Paul Wouters (16:15-16:25)
    - draft-sprasad-ipsecme-labeled-ipsec
  - Diet ESP (10 min) – Daniel Migault (16:25-16:35)
    - draft-mglt-ipsecme-diet-esp
  - Controller IKE (10 min) – David Carrel (16:35-16:45)
    - draft-carrel-ipsecme-controller-ike

WG Status Report

RFC Ed queue:

- draft-ietf-ipsecme-eddsa

Publication requested, but has some issues:

- draft-ietf-ipsecme-split-dns

WGLC done:

- draft-ietf-ipsecme-implicit-iv

Ready for WGLC:

- draft-ietf-ipsecme-qr-ikev2

Discussion of Current Work

- Split-dns (10 min) – Tommy Pauly
  - draft-ietf-ipsecme-split-dns
- Auxiliary Exchange in the IKEv2 Protocol (15 min) - Valery Smyslov
  - draft-smysov-ipsecme-ikev2-aux
- Postquantum Key Exchange to IKE (15 min) – Scott Fluhrer
  - draft-tjhai-ipsecme-hybrid-qske-ikev2
- Labeled IPsec (10 min) - Paul Wouters
  - draft-sprasad-ipsecme-labeled-ipsec
- Diet ESP (10 min) – Daniel Migault
  - draft-mglt-ipsecme-diet-esp
- Controller IKE (10 min) – David Carrel
  - draft-carrel-ipsecme-controller-ike

Split-dns

- Issue raised by AD hopefully solved
  - https://www.ietf.org/rfcdiff?url2=draft-ietf-ipsecme-split-dns-09

Split-dns changes

IKE clients **MUST** use a preconfigured whitelist of domain names for which it will allow INTERNAL_DNSSEC_TA updates.

The DNS root zone (".") **MUST NOT** be whitelisted.

Any updates to this whitelist of domain names **MUST** happen via explicit human interaction to prevent invisible installation of trust anchors.

IKE clients **SHOULD** accept any INTERNAL_DNSSEC_TA updates for subdomain names of the whitelisted domain names. For example, if "example.net" is whitelisted, then INTERNAL_DNSSEC_TA received for "antartica.example.net" **SHOULD** be accepted.

IKE clients **MAY** interpret an INTERNAL_DNSSEC_TA for domain that was not preconfigured as an indication that it needs to update its IKE configuration (out of band). The client **MUST NOT** use such a INTERNAL_DNSSEC_TA to reconfigure its local DNS settings.

Labeled IPsec

- Discussion

Open Discussion

- Other points of interest?