IPsecME IETF 108

Time: Tuesday, 28-Jul-2020, at 11:00-12:40 UTC

Agenda:

- 11:00-11:05 - Note Well, technical difficulties and agenda bashing
- 11:05-11:10 - Document status (chairs)
- 11:10-11:25 - draft-smyslov-ipsecme-rfc8229bis (Valery/Tommy)
- 11:25-11:35 - draft-btw-add-ipsecme-ike-00 (Valery)
- 11:35-11:45 - draft-smyslov-ipsecme-ikev2-auth-announce (Valery)
- 11:45-12:00 - Proposed improvements to ESP (Michael Rossberg)
- 12:00-12:15 - IPTFS (Christian Hopps)
- 12:15-12:30 - YANG model for IPTFS (Christian Hopps)
- 12:30-12:40 - AOB + Open Mic

Note Well, technical difficulties and agenda bashing

Chairs (5min)

No Edits

Document status

chairs (5min)

*-implicit-Iv published as RFC8750
*-qr-ikev2 published as RFC8784

*-ipv6-ipv4-codes publication requested

draft-smyslov-ipsecme-rfc8229bis (TCP encap of IKE/IPsec)

Valery/Tommy (15min)

Slides link: https://www.ietf.org/proceedings/108/slides/slides-108-ipsecme-rfc8229bis-00

Paul Wouters: What are the kernel implications? And does this allow for smaller IPsec/ESP Packets?
Valery: Text is a bit short, TCP stream packets will have same class

Paul: What Interop testing has been done?
Valery: Tested with Apple, Cisco, libreswan

Piannissimo Hum for who has read the draft

Paul: Good idea to adopt, found issues that would be good to incorporate in draft

Yoav: Will take to list if we need an update to 8229 and if this is the right starting point.

draft-btw-add-ipsecme-ike-00 (IKEv2 config for Encrypted DNS)

Valery (10min)

Slides link: https://www.ietf.org/proceedings/108/slides/slides-108-ipsecme-ikev2-configuration-for-encrypted-dns-00

Paul: What to do outside of VPN tunnel seems out of scope? (regarding Scope bit)

Valery: Still an interesting subject

Ben (AD): (missed first point Belongs in ADD?) Slide with attribute format, for DoH, need to provide URI template

Valery: Presentation also requested in ADD, but didn't have room in agenda. Re: URI, will be covered in DoH clarifications (?)

Ben: When DoQ arrives may need additional work

Tero: Add configuration attributes, less internal strucutre, more higher level structure

Yoav (participant): Missing motivation from draft Moving towards encrypted world, don't want to force people to keep insecure DNS just for legacy IKEv2 server

Valery: That is one of the motivations; users won't see this, but it is useful.

Tirumaleswar Reddy: URL can be discovered another way

Benedict Wong: My understanding is that in some cases we need a hostname to do validation of the DoT server

Tirumaleswar: This only supports PKI-based verification, so we can verify based on sent certificate.

Yoav: Calling for adoption?

Valery: ADD Primary target for adoption, ipsecme is just informational, if there is interest it could persist in this WG, but not yet.

Tirumaleswar: Couple more revisions necessary, extension to IKE, want to make sure both working groups are aware of work

Ben (AD): If ipsecme was concerned by the work, or on the other hand thinks it makes sense, it's good information for ADD to have

draft-smyslov-ipsecme-ikev2-auth-announce

Valery (10min)

Slides link: https://www.ietf.org/proceedings/108/slides/slides-108-ipsecme-announcing-supported-authentication-methods-in-ikev2-00

Paul: Good idea, unclear where complexity might be, in the past migration between methods (null -> something else) needed a ppk hack - sending two auth payloads

Tero (participant): Could have one part negotiate the algorithm, and the second part to negotiate the algorithm ids for CAs in the certreq

Yoav: will take a call for adoption to the list

Proposed improvements to ESP

Michael Rossberg (15min)

Slides link: https://www.ietf.org/proceedings/108/slides/slides-108-ipsecme-proposed-improvements-to-esp-01

Yoav (?): Discussion happening on list and in jabber. Informational would be wrong, changes packet on wire, so experimental or standards track if anything

Summary of questions and comments from the jabber:

- Yoav: Some firewalls would be very upset about this packet format, because it looks like every packet is retransmission.
- Paul: so flip sender/window id with sequence number

- Chopps: andeven put the higher order after lower order so stays exactly the same as before
- Scott Fluhrer: In addition, each sending id/window id has its own replay window, does that mean that the receiver needs to track 4 billion antireplay windows?
- Scott: Also, it wouldn't be secure with CBC
- Paul: It drops all non-AEAD, which we should do anyways
- Scott: You also lose the multitarget protection with GCM by not including the 32 bits of key-derived nonce
- chopps: The sender id is really a mcast thing, so it reduces to 64k
- Scott: Does the receiver need to track a antireplay window for each multicast sender?
- Yaov: Yes
- Scott: I can't see how that can work on a decryptor that can't dynamically allocate memory
- Bob Moskowitz: Would need a change to robust header compression so that smaller seq# for constrained links?
- Valery: This proposal lacks enough generality to replace ESP - it considers very small set of ciphers and use cases
- Paul: and we might as well throw in a discussion of implicit IV if we are updating ESP to v4
- Yoav: @Valery: doesn't it use all the ciphers that people care about now? Consider that TLS 1.3 has about two ciphers (plus another 1 for IOT).
- Valery: In addition, many things it aims for can be achieved using ESP. Even replay protection for multicast (with some limitations).
- Steffen Klassert: Get rid of the trailer would be nice from implementation point of view
- Valery: @yoav, No, it doesn't work with CBC at all. Moreover, if IV is somehow structured, it won't work too
- Yoav: TLS 1.3 doesn't support CBC either.
- Valery: I understand, but what if tomorrow a new cipher mode appear that is superior to GCM and will require some special form of IV? The problem is that this design requires IV to be in a particular form. If cipher requires other form, it'll fail

Tero: Not in charter, this is a big change. See if it is a good idea first before taking to much time discussing and writing

IPTFS – draft-ietf-ipsecme-iptfs-01

Christian Hopps (15min)

Slides link: https://www.ietf.org/proceedings/108/slides/slides-108-ipsecme-ip-traffic-flow-security-00

Yoav: Hasn't gotten much review, WGLC is one way, but don't know if it is the best way. Requesting transport area early may be a good way too.

Tero: Might be hard to get another protocol number.

Lou: Getting a protocol number shouldn't be a big deal; many can be deprecated.

Ben: Please fill out the official early-allocation form request.

Agreed on sending this out for transport area early review.

YANG model for IPTFS – draft-fedyk-ipsecme-yang-iptfs-00

Christian Hopps (15min)

Slides link: https://www.ietf.org/proceedings/108/slides/slides-108-ipsecme-yang-model-for-ip-traffic-flow-security-00

Tero: SDN YANG models generally work in two mode, either IKE-less, where it configures IPsec SAs, or in IKE mode where it does not touch IPsec SAs, as IKE configures them, so they wanted to keep the configuration clear which parts they are configuring.

Christian: Also operational state, even if not configured via YANG

Tero: If we could consolidate on a single YANG model, that would be ideal (such as I2NFS)

Yoav: Per chat, would benefit from a YANG Dr. review

Lou: Would benefit from another review, per datatracker, latest draft needs another review.

AOB + Open Mic

all (10min)

Paul: Labeled IPsec still in review. Graveyard draft still in limbo

Tero: Take to list; a few of these can go to WGLC, but should check with AD first.

Tero: I think we need to have interm meeting about the ESP. We cut the discussion out from here, as it would have taken the rest of the time, but we should have separate interm just for it.

Action Items for the Chairs

1. Consensus Call on the list about whether RFC 8229 needs an update and whether draft-smyslov-ipsecme-rfc8229bis isa good starting point.
2. Call for adoption for draft-smyslov-ipsecme-ikev2-auth-announce. Not clear if it falls under the general “maintenance” task in the charter or whether it will need a charter revision.
3. Set up a virtual interim meeting about Michael Rossberg’s proposed improvements to ESP. This is definitely not in our charter, but spending an interim meeting with proponents and others to determine if this is worthwhile seems like a good idea. A lively discussion is already happening on-list.
4. IPTFS - Handle request for allocation of IP protocol number
5. IPTFS - Early transport directorate review.
6. YANG for IPTFS (and IPsec in general) - need to figure out interaction with I2NSF document.
7. Graveyard + Labeled IPsec - Perhaps go to WGLC.