IP Security Maintenance and Extensions (IPsecME) WG

IETF 113, Friday, March 25th, 2022

Chairs: Tero Kivinen
Yoav Nir

Responsible AD: Benjamin Kaduk

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: https://meetings.conf.meetecho.com/ietf113/?group=ipsecme&short=&item=1

Notes: https://notes.ietf.org/notes-ietf-113-ipsecme

Agenda

- Note Well, technical difficulties and agenda bashing – Chairs (5 min) (11:30-11:35)
- Document Status – Chairs (10 min) (11:35-11:45)
- Work items
  - Group Key Management using IKEv2 – Valery Smyslov (20 min) (11:45-12:05)
  - IKEv2 Optional SA&TS Payloads in Child Exchange – William Panwei(10 min) (12:05-12:15)
- AOB + Open Mic (75 min) (12:15-13:30)

WG Status Report

Publication requested:

- draft-ietf-ipsecme-ikev2-intermediate
- draft-ietf-ipsecme-iptfs
- draft-ietf-ipsecme-yang-iptfs
- draft-ietf-ipsecme-mib-iptfs

Waiting for write-up / Chair review:

- draft-ietf-ipsecme-ikev2-multiple-ke
- draft-ietf-ipsecme-ikev1-algo-to-historic
- draft-ietf-ipsecme-labeled-ipsec
- draft-ietf-ipsecme-rfc8229bis

Work in progress:

- draft-ietf-ipsecme-g-ikev2
- draft-ietf-ipsecme-add-ike
- draft-ietf-ipsecme-auth-announce

More detailed status of drafts in progress

- Group Key Management using IKEv2
  - draft-ietf-ipsecme-g-ikev2
  - Still would like to get more reviews
  - Still in WGLC, will close it after this meeting.

Presentations

- Group Key Management using IKEv2 – Valery Smyslov
- IKEv2 Optional SA&TS Payloads in Child Exchange – William Panwei

Presentations

- **Group Key Management using IKEv2 – Valery Smyslov**
- IKEv2 Optional SA&TS Payloads in Child Exchange – William Panwei

Group Key Management using IKEv2

draft-ietf-ipsecme-g-ikev2

Valery Smyslov
ELVIS-PLUS

Brian Weis
Independent

IETF 113

Document Status

- Has been in development for several years
  - few implementations of early draft versions exist
- Has been adopted by IPSECME WG in 2019
- Version -01 (July 2020): major rewrite
- Version -02 (January 2021): minor update
- Version -03 (July 2021): minor update
- Version -04 (January 2022): no changes
- **Version -05 (March 2022): major update as result of WGLC comments**
  - Reviews are needed

Issues Resolved in -05

- Terminology section added
- It is clarified that IKE_AUTH and GSA_AUTH exchanges are treated equally with regard to IKEv2 extensions
- Keys used inside Rekey SA are renamed from SK_a/SK_e/SK_w to GSK_a/GSK_e/GSK_w
- Changing Authentication method and authentication key is prohibited in rekey operations, as well as changing Key Management method
- Using SIDs is clarified (in particular how the GCKS handles the situation when it runs out of available SIDs)
- Consistency of the document is improved, a lot of clarifications is added

Unresolved Issues

- Changing public key in rekey operations
- Using ports
- Unregistration of a GM
- AUTHORIZATION_FAILED vs REGISTRATION_FAILED
- Explicit PSK authentication
- ESN
- Integration with RFC 8784
- Using Tunnel Mode
- UDP encapsulation
- Transport mode signaling

Changing Public Key in Rekey operations

- Changing Authentication method and authentication key is prohibited in rekey operations, including changing public key for digital signatures (if they are used for authentication of multicast rekeys)
  - Is it OK?

Using Ports

- For compatibility with GDOI the draft allows using port 848. Standard IKEv2 ports 500/4500 are also allowed, as well as using TCP.
  - Should the unicast IKE SA switch from port 848 to 4500 if NAT is detected?
    - Yes

Unregistration of GM

- Is it needed?
  - No strict opinion. Explicit unregistering of the GM can save some GCKS's resources, e.g. in case of LKH. On the other hand, in most cases GCKS operations don't depend on the population of the group.

AUTHORIZATION_FAILED vs REGISTRATION_FAILED

- Which notification to use in which case?
  - AUTHORIZATION_FAILED is used when something is wrong with the GM and REGISTRATION_FAILED if something is wrong with the group (e.g. the capacity of the group is exceeded)

Is Explicit PSK Authentication needed?

- The draft defines two authentication modes based on symmetric shared secret for multicast rekey operations (besides authentication with digital signatures). When PSK authentication is explicit, a dedicated shared secret is transferred to GMs at the time of registration and is used across all rekey operations. Implicit authentication relies on the ability for GMs to decrypt and verify ICV of the received multicast packet (i.e. a knowledge of message protection keys which change with every rekey operation).
  - No strict opinion

ESN

- High-order 32 bits of extended sequence numbers are never transmitted in IPsec, it makes using ESN in multicast Data-Security SAs problematic, because GMs that join group long after it was created have to somehow learn the current high order 32 bits of ESN for each sender in the group. The algorithm for doing this described in RFC4302 and RFC4303 is resource-consuming
  - SHOULD NOT be used?
  - MUST NOT be used?

Integration with RFC 8784

- When PPK is used GSK_w is derived from SK_d, so an attacker cannot learn the multicast SA keys, but authentication of the keys is performed on IKE message level, so an attacker can tamper them, if it is able to break DH in real time, and can also see all the other stuff (like group policy). Is it an important threat to justify developing draft-smyslov-ipsecme-ikev2-qr-alt?
  - No strict opinion

Tunnel Mode

- RFC 5374 (Multicast Extensions to the Security Architecture for the Internet Protocol) allows both tunnel and transport modes for multicast SA. However, for tunnel mode it defines a special mode called Tunnel Mode with Address Preservation, when IP addresses from the inner IP header are copied to the outer one.
  - It seems that this mode has little value, but consumes resources; the only reason to use it – if SGW is participating in the group; how GCKS knows if this is the case?
    - Is it preconfigured?
  - Both dst and src addresses can be preserved, however the preservation of src address is optional
    - Who will control it – SGW or GCKS?

UDP Encapsulation

- Is UDP encapsulation needed for multicast Data-Security SAs? If yes, then how to signal it? Explicitly (e.g. add new Transform Type) or implicitly by specifying destination port 4500?
  - No strict opinion

Transport Mode Signaling

GSA may have some IPsec SAs created in tunnel mode and some – in transport mode. How to indicate which SAs are created in which mode?

- Change semantics of USE_TRANSPORT_MODE when it is used in the context of G-IKEv2
  - Protocol and SPI fields are used to indicate which SAs use transport mode
  - multiple instances can be sent if multiple SAs use transport mode
  - no update to RFC7296 is needed, since the context is clear
- Add new notification (e.g. GSA_USE_TRANSPORT_MODE)
- Add new transform (e.g. Encapsulation Mode) in GSA payload
- Prohibit policy when different IPsec SAs have different encapsulation modes in a single GSA payload and use USE_TRANSPORT_MODE without changing its semantics

Thank you!

- Comments?
- Questions?
- Please review the document

Presentations

- Group Key Management using IKEv2 – Valery Smyslov
- **IKEv2 Optional SA&TS Payloads in Child Exchange – William Panwei**

IKEv2 Optional SA&TS Payloads in Child Exchange

https://datatracker.ietf.org/doc/draft-kampati-ipsecme-ikev2-sa-ts-payloads-opt/

Sandeep Kampati (Huawei)

Wei Pan (Huawei)

Paul Wouters (Aiven)

Meduri Bharath (Mavenir)

Meiling Chen (CMCC)

Michael Richardson (SSE)

IETF 113

March 2022

Solution Recap:

- Negotiation of Support for OPTIMIZED REKEY

```
Initiator                           Responder
-----------------------------------------------------------------------
HDR, SK {IDi, [CERT,] [CERTREQ,]
    [IDr,] AUTH, SAi2, TSi, TSr,
    N(OPTIMIZED_REKEY_SUPPORTED)} -->
                                    <-- HDR, SK {IDr, [CERT,] AUTH,
                                        SAr2, TSi, TSr,
                                        N(OPTIMIZED_REKEY_SUPPORTED)}
```

- Optimized Rekey of the IKE SA

```
Initiator                           Responder
-----------------------------------------------------------------------
HDR, SK {N(OPTIMIZED_REKEY,newSPIi),
    Ni, KEi} -->
                                    <-- HDR, SK {N(OPTIMIZED_REKEY,newSPIr),
                                        Nr, KEr}
```

Note: The old SPI is from the IKE header.

- Optimized Rekey of Child SAs

```
Initiator                           Responder
-----------------------------------------------------------------------
HDR, SK {N(REKEY_SA,oldSPI), N(OPTIMIZED_REKEY,newSPIi),
    Ni, [KEi,]} -->
                                    <-- HDR, SK {N(OPTIMIZED_REKEY,newSPIr),
                                        Nr, [KEr,]}
```

Updates from -07 to -08

- Most are editorial changes
- Clearly show how new and old SPIs are included in the Child Exchange
  - At rekeying IKE SA:
    - The oldSPI is included in the IKE header.
    - The newSPIs are respectively included in the initiator and responder's OPTIMIZED_REKEY payloads.
  - At Rekeying Child SA:
    - The oldSPI is included in the initiator’s REKEY_SA payload.
    - The newSPIs are respectively included in the initiator and responder's OPTIMIZED_REKEY payloads.

Next Step

- Ask for WG adoption
  - The authors believe current version is clear and mature.

Open Discussion

- Other points of interest?