IKEv2 Optional SA&TS Payloads in Child Exchange

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

Sandeep Kampati (Microsoft)

Wei Pan (Huawei)

Paul Wouters (Aiven)

Meduri Bharath (Mavenir)

Meiling Chen (CMCC)

IETF 115

November 2022

Background:

- In RFC 7296 Section 2.8, it says:
  - `... Note that, when rekeying, the new`
  - `Child SA SHOULD NOT have different Traffic Selectors and algorithms`
  - `than the old one.`
- So, omitting the SA&TS payloads during rekey:
  - doesn’t violate RFC 7296,
  - can save the bandwidth in wire,
  - and can reduce the CPU operations.

Solution Recap (same as IETF 113):

- 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 current SPI is from the IKE header.

- Optimized Rekey of Child SAs

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

Updates from -08 to -10

- Typos fixed:
  - TS payloads are misspelled as TA payloads.

IETF 113 IPsecME report

[saag] IPsecME WG report for SAAG

Tero Kivinen <kivinen@iki.fi> | Wed, 23 March 2022 13:08 UTC | Show header

IPsecME will be meeting on Friday after the saag so I updated the status on the datatracker to describe the current status (https://datatracker.ietf.org/group/ipsecme/about/status/).

Intermediate draft is now approved by the IESG and is now in the RFC Editor queue. Publication has been requested for IPTFS drafts (base draft, and yang and mib drafts), and the TCP Ecnapsulation (rfc8229bis) draft. Labeled IPsec and Deprecation of IKEv1 and obsoleted algorithms drafts are ready for publication and will be submitted to the IESG immediately after this IETF. Multiple Key Exchanges draft should also be ready for publication.

Group Key Management using IKEv2 has received some reviews during the WGLC, and should be ready for publication now. IKEv2 configuration for Encrypted DNS and Announcing Supported Authentication Methods in IKEv2 drafts are adopted as WG drafts.

There has been some work on the Optional SA & TS Payload in Child Exchange, and it might be ready to be adopted as WG draft.

There has not been that much happening with other new work, like modifying the base IKEv2 payload format, both to make it more compact for constrained devices, and allow it to go over 64kB payload limit.

IETF 114 IPsecME report

[saag] IETF 114 IPsecME report

Tero Kivinen <kivinen@iki.fi> | Tue, 26 July 2022 02:23 UTC | Show header

This status has also be uploaded to the datatracker at
https://datatracker.ietf.org/group/ipsecme/about/status/

Intermediate draft published as RFC 9242. Publication has been requested for IPTFS (base draft, and yang and mib drafts), TCP Encapsulation (rfc8229bis), multiple ke, and deprecation of IKEv1 and obsolete algorithms drafts. Labeled IPsec is ready for publication and will be submitted to the IESG immediately after this IETF.

Group Key Management still would benefit from more reviews, but we might go forward with anyways. IKEv2 configuration for Encrypted DNS should be ready for WGLC, but Announcing Supported Authentication Methods in IKEv2 needs more reviews before that.

The Optional SA & TS Payload in Child Exchange, and multi sa performance should be ready for WG adoption calls.

Quite a lot of charter items have been finished, so we should start working on to do rechartering, and clear out old things already finished, and add some new work to the charter. Most likely try to work on charter update in November IETF meeting and do rechartering after that.

IETF 115 IPsecME report

- “must be ready for WG adoption calls”?

Next Steps

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