Workgroup: Network Working Group
Internet-Draft:
draft-liu-ipsecme-ikev2-rekey-redundant-sas-00
Published: 21 November 2021
Intended Status: Informational
Expires: 25 May 2022
Authors: D. Liu, Ed. D. Migault, Ed. C. Zhang
Ericsson Ericsson Ericsson

IKEv2 Rekey Priority Extension

Abstract

This document defines the Internet Key Exchange Version 2 (IKEv2) Rekeying Priority extension that enables to agree roles for the next rekey of the child SAs and as such optimize IKEv2 rekey negotiation.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 25 May 2022.

Table of Contents

1. Introduction

The IKEv2 protocol supports rekey mechanism for IKE Security Association (SA) and Child SA, but may result in redundant SAs ([RFC7296], section 2.8.1) when both peers start rekeying at the same time. In such case IKEv2 selects the SA created with the lowest of the four nonces and the redundant SA SHOULD be deleted by the endpoint that created it.

Among the standards, frequent rekeying is highly recommended, but such an approach can be non optimal when SA are frequently rekeys as SAs are unnecessary computed and adds an additional IKEv2 exchange.

So this document defines the Rekeying Priority in IKEv2 extension which enables to agree roles for rekeying of child SAs and optimize IKEv2 rekey negotiation.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] [RFC8174].

3. Rekeying Priority Notify Message Types

Figure 2 illustrates the Notify Payload packet format as described in Section 3.10 of [RFC7296] with a 4 byte Rekeying Priority value as Notification Data used for the REKEY_PRI notification.

The REKEY_PRI notification is used in an IKEv2 exchange of type IKE_AUTH and CREATE_CHILD_SA.

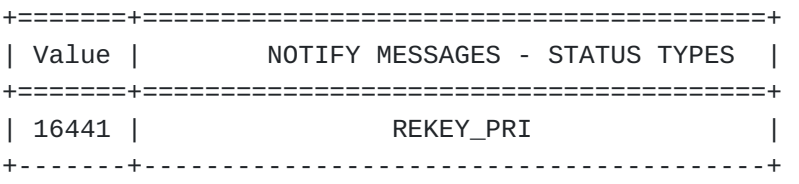

Figure 1: REKEY_PRI Notify Message Type Value

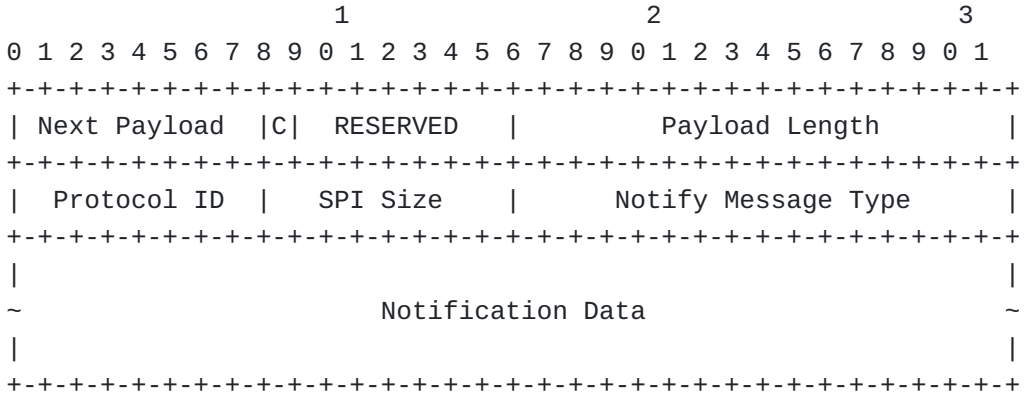

Figure 2: REKEY_PRI Notify Message Format

*Next Payload - N(41), indicate this is Notify payload.

*Protocol ID - 0, indicate this payload is not concerning the SPI.

*SPI Size - 0, indicate this payload is not concerning the SPI.

*Notify Message Type - REKEY_PRI(16441).

*Notification Data - 4 octets for REKEY_PRI, see Figure 3:

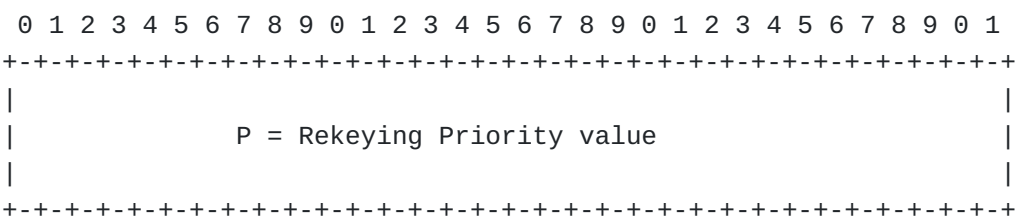

Figure 3: Notification Data for REKEY_PRI

A peer supporting rekey SHOULD put a randomly selected value that is non null for the Rekeying Priority value. For example, the random value could be generated from some local unique information like hardware serial number or MAC. A random value insure an uniform distribution of the roles.

A value set to zero indicates the peer does not support rekey. Although disabling the rekeying is not recommended in [RFC7296]

section 2.8, disabling rekeying is implemented by most of the products.

A peer supporting the Rekeying Priority Extension SHOULD NOT set the Rekeying Priority value to zero unless it does not support rekey.

An initiator supporting the Rekeying Priority Extension SHOULD send a Priority Notify Payload in its IKE_AUTH and CREATE_CHILD_SA message. A responder supporting the Rekeying Priority Extension receiving a Priority Notify Payload SHOULD respond with a Priority Notify Payload. When initiator and responders have received the Rekeying Priority Extension, the sender of the highest Rekeying Priority value is expected to be assigned the initiator role of the next rekey. The rekey is expected to be performed as recommended in [RFC7296] a reasonable value is to perform the rekey at XXX % of the SA life time. When that trigger has been reach the peer being assigned the responder role MAY proceed to a rekey as defined in [RFC7296].

Maybe section 4 and 5 could be example.

4. IKE_SA_INIT Stage

No changes have been made to IKE_SA_INIT in this document. IKE_SA_INIT is described here (see [RFC7296] Section 1.2) for the sake of logical coherence and completeness and to make it easier for the reader to understand.

The initial exchanges are shown as Figure 4:

Figure 4: IKE_SA_INIT Exchanges

5. IKE_AUTH Stage

When IKE_SA_INIT is completed, the IKE_AUTH message exchanges will take place and the NOTIFY message "REKEY_PRI" should be added to IKE_AUTH, as shown below:

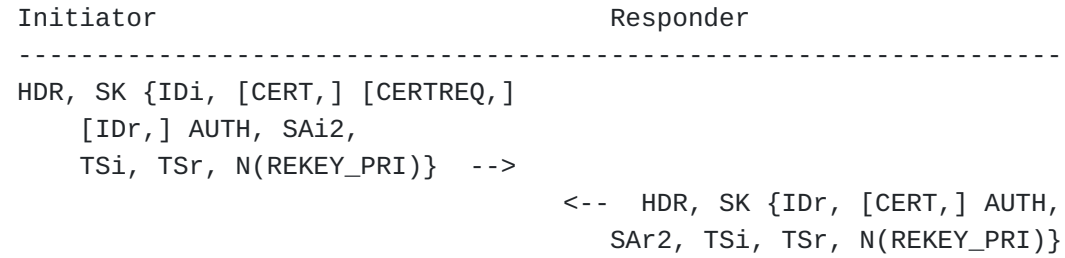

Figure 5: IKE_AUTH Exchanges

The initiator begins negotiation of a Child SA using the SAi2 payload, and the responder completes negotiation of a Child SA with the additional fields.

At this point, the two endpoints get the Rekeying Priority of the opposite end via the IKE_AUTH message, and can decide which endpoint to trigger rekeying using the mechanism described in Section 3.

6. CREATE_CHILD_SA Stage

If creating the Child SA during the IKE_AUTH exchange fails for some reason, the IKE SA is still created as usual and use CREATE_CHILD_SA message to create new Child SA ([RFC7296] Section 1.2), the exchanges are as follow:

Figure 6: CREATE_CHILD_SA Exchanges for Create Child SA

The Rekeying Priority configuration may be changed after the SA is set up. In this case, the Rekeying Priority should be added to the CREATE_CHILD_SA message in order to renegotiate which end to trigger rekeying. This allows both sides to renegotiate the Rekeying Priority the next time they exchange the CREATE_CHILD_SA message (for example, rekeying will be processed by the CREATE_CHILD_SA message).

The CREATE_CHILD_SA request for rekeying an IKE SA is:

```
 Initiator                              Responder
 ------------------------------------------------------------------
 HDR, SK {SA, Ni, [KEi,]
 N(REKEY_PRI)}       -->
                                    <--  HDR, SK {SA, Nr, [KEr,],
                                             N(REKEY_PRI)
```

Figure 7: CREATE_CHILD_SA Exchanges for IKE SA Rekeying

The CREATE_CHILD_SA request for rekeying an Child SA is:

```
 Initiator                              Responder
 ------------------------------------------------------------------
 HDR, SK {N(REKEY_SA),
 SA, Ni, [KEi,],
 TSi, TSr,
 N(REKEY_PRI)}       -->
                                    <--  HDR, SK {SA, Nr, [KEr,],
                                               TSi, TSr,
                                             N(REKEY_PRI)
```

Figure 8: CREATE_CHILD_SA Exchanges for Child SA Rekeying

7. Security Considerations

This document defines new IKE Notify message types that are naturally protected by the IKE encryption mechanism when the payloads are applied.

So there is no security problem or potential risk.

8. IANA Considerations

ANA need to update the "IKEv2 Notify Message Types - Status Types" registry (available at https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-16) with the following definition:

Value	NOTIFY MESSAGES - STATUS TYPES
16441	REKEY_PRI

Figure 9

9. Acknowledgements

This document reproduces some parts of the similar IKEv2 document ([RFC7296]).

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

10.2. Informative References

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, DOI 10.17487/RFC5226, May 2008, <https://www.rfc-editor.org/info/rfc5226>.

Authors' Addresses

Daiying Liu (editor)
Ericsson

Email: harold.liu@ericsson.com

Daniel Migault (editor)
Ericsson

Email: daniel.migault@ericsson.com

Congjie Zhang
Ericsson

Email: congjie.zhang@ericsson.com