IPSECME Working Group
Internet-Draft
Intended status: Standards Track
Expires: 24 April 2023

S. Kampati
Microsoft
W. Pan
Huawei
P. Wouters
Aiven
M. Bharath
Mavenir
M. Chen
CMCC

21 October 2022

IKEv2 Optional SA&TS Payloads in Child Exchange
draft-kampati-ipsecme-ikev2-sa-ts-payloads-opt-10

Abstract

This document describes a method for reducing the size of the Internet Key Exchange version 2 (IKEv2) CREATE_CHILD_SA exchanges used for rekeying of the IKE or Child SA by replacing the SA and TS payloads with a Notify Message payload. Reducing size and complexity of IKEv2 exchanges is especially useful for low power consumption battery powered devices.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-kampati-ipsecme-ikev2-sa-ts-payloads-opt/.

Discussion of this document takes place on the ipsec Working Group mailing list (mailto:ipsec@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/ipsec/. Subscribe at https://www.ietf.org/mailman/listinfo/ipsec/.

Source for this draft and an issue tracker can be found at https://github.com/mcr/ipsecme-ikev2-sa-ts-payloads.git.

Status of This Memo

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

This Internet-Draft will expire on 24 April 2023.

Copyright Notice

Table of Contents

1. Introduction

The Internet Key Exchange protocol version 2 (IKEv2) [RFC7296] is used to negotiate Security Association (SA) parameters for the IKE SA and the Child SAs. Cryptographic key material for these SAs have a limited lifetime before it needs to be refreshed, a process referred to as "rekeying". IKEv2 uses the CREATE_CHILD_SA exchange to rekey either the IKE SA or the Child SAs.

When rekeying, a full set of negotiation parameters are exchanged. However, most of these parameters will be the same as before, and some of these parameters MUST NOT change.

For example, the Traffic Selector (TS) negotiated for the new Child SA MUST cover the Traffic Selectors negotiated for the old Child SA. And in practically all cases, a new Child SA does not need to cover a wider set of Traffic. In the rare case where this would be needed, either a standard rekey could be used or a new Child SA could be negotiated followed by a deletion of the replaced Child SA.

Similarly, IKEv2 states that the cryptographic parameters negotiated for rekeying SHOULD NOT be different. This means that the security properties of the IKE or Child SA in practise do not change during a typical rekey.

This document specifies a method to omit these parameters and replace them with a single Notify Message declaring that all these parameters are identical to the originally negotiated parameters.

Large scale IKEv2 gateways such as Evolved Packet Data Gateway (ePDG) in 4G networks or Centralized Radio Access Network (cRAN/Cloud) gateways in 5G networks typically support more than 100,000 IKE/IPsec connections. At any point in time, there will be hundreds or thousands of IKE SAs and Child SAs that are being rekeyed. This takes a large amount of bandwidth and CPU power and any protocol simplification or bandwidth reducing would result in a significant resource saving.

For Internet of Things (IoT) devices which utilize low power consumption technology, reducing the size of the CREATE_CHILD_SA exchange for rekeying reduces its power consumption, as sending bytes over the air is usually the most power consuming operation of such a device. Reducing the CPU operations required to verify the rekey exchanges parameters will also save power and extend the lifetime for these devices.

When using identical parameters for the IKE SA or Child SA rekey, the SA and TS payloads can be omitted thanks to the optimization defined in this document. For an IKE SA rekey, instead of the (large) SA payload, only a Key Exchange (KE) payload and a new Notify Type payload with the new SPI are required. For a Child SA payload, instead of the SA or TS payloads, only an optional nonce payload (when using PFS) and a new Notify Type payload with the new SPI are needed. This makes the rekey exchange packets much smaller and the peers do not need to verify that the SA or TS parameters are compatible with the old SA parameters.

2. Conventions Used in This Document

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Negotiation of Support for OPTIMIZED REKEY

To indicate support for the optimized rekey negotiation, the initiator includes the OPTIMIZED_REKEY_SUPPORTED notify payload in the IKE_AUTH exchange request. During this initial key request, the entire SA and TS payloads are included as normal. A responder that supports the optimized rekey exchange includes the OPTIMIZED_REKEY_SUPPORTED notify payload in its response. Note that the notify indicates support for optimized rekey for both IKE and Child SAs.

A responder that does not support the optimized rekey exchange processes the SA and TS payloads as normal, and does not include the new Notify. As per regular IKEv2 processing, a responder that does not recognize this new Notify, MUST ignore the notify. Responders may have been administratively configured with the optimization turned off for local reasons. The absense of the Notify indicates to the initiator that the optimization is not available, and normal, full rekey should be done.

When a peer wishes to rekey an IKE SA or Child SA, it MAY use the optimized rekey method during the CREATE_CHILD_SA exchange. If both peers have exchanged OPTIMIZED_REKEY_SUPPORTED notifies, peers SHOULD use the optimized rekey method for rekeys. Non-optimized, regular rekey requests MUST always be accepted.

The IKE_AUTH message exchange in this case is shown below:

```
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)}
```

4. Optimized Rekey of the IKE SA

The initiator of an optimized rekey request sends a CREATE_CHILD_SA payload with the OPTIMIZED_REKEY notify payload containing the new Security Parameter Index (SPI) for the new IKE SA. It omits the SA payload.

The responder of an optimized rekey request replies with an included OPTIMIZED_REKEY notify with its new IKE SPI and also omits the SA payload.

Both parties send their nonce and KE payloads just as they would do for a regular IKE SA rekey.

Using the old SPI from the IKE header and the two new SPIs respectively from the initiator and responder's OPTIMIZED_REKEY payloads, both parties can perform the IKE SA rekey operation.

The CREATE_CHILD_SA message exchange in this case is shown below:

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

5. Optimized Rekey of Child SAs

The initiator of an optimized rekey request sends a CREATE_CHILD_SA payload with the OPTIMIZED_REKEY notify payload containing the new Security Parameter Index (SPI) for the new Child SA. It omits the SA and TS payloads. If the current Child SA was negotiated with Perfect Forward Secrecy (PFS), a KEi payload MUST be included as well. If no PFS was negotiated for the current Child SA, a KEi payload MUST NOT be included.

The responder of an optimized rekey request performs the same process. It includes the OPTIMIZED_REKEY notify with its new IKE SPI and omits the SA and TS payloads. Depending on the PFS negotiation of the current Child SA, the responder includes a KEr payload.

Both parties send their nonce payloads just as they would do for a regular Child SA rekey.

Using the old SPI from the REKEY_SA payload and the two new SPIs respectively from the initiator and responder's OPTIMIZED_REKEY payloads, both parties can perform the Child SA rekey operation.

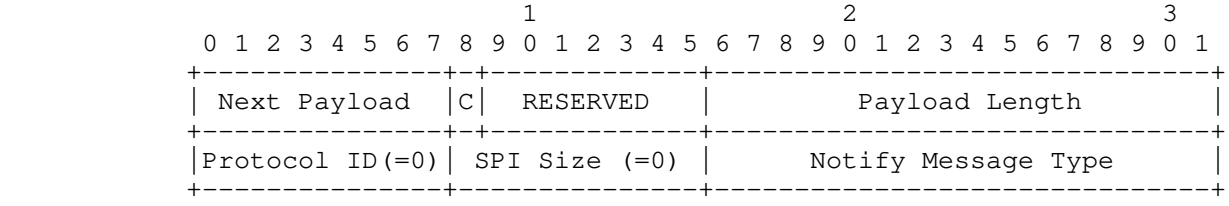
The CREATE_CHILD_SA message exchange in this case is shown below:

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

6. Payload Formats

6.1. OPTIMIZED_REKEY_SUPPORTED Notify

The OPTIMIZED_REKEY_SUPPORTED Notify Message type notification is used by the initiator and responder to indicate their support for the optimized rekey negotiation.



* Protocol ID (1 octet) - MUST be 0.

* SPI Size (1 octet) - MUST be 0, meaning no SPI is present.

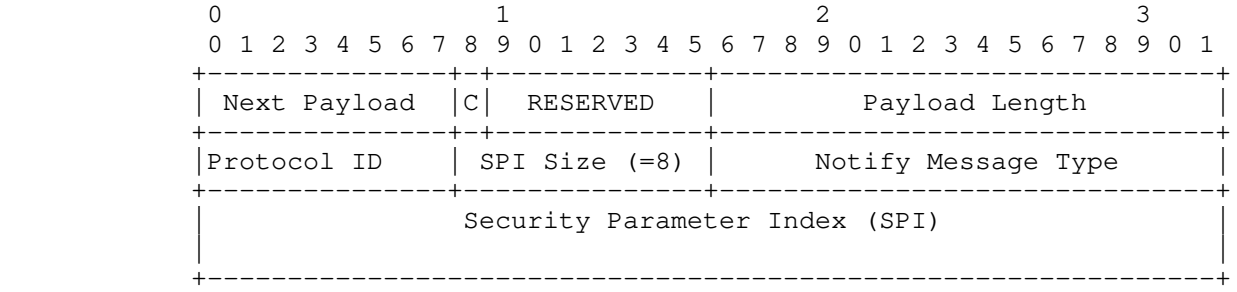
* Notify Message Type (2 octets) - MUST be set to the value TBD1.

This Notify Message type contains no data.

The Critical bit MUST be 0. A non-zero value MUST be ignored.

6.2. OPTIMIZED_REKEY Notify

The OPTIMIZED_REKEY Notify Message type is used to perform an optimized IKE SA or Child SA rekey.



* Protocol ID (1 octet) - For an IKE SA rekey, this field MUST contain (1). For Child SAs, this field MUST contain either (2) to indicate AH or (3) to indicate ESP.

* SPI Size (1 octet) - MUST be 8 when rekeying an IKE SA. MUST be 4 when rekeying a Child SA.

* Notify Message Type (2 octets) - MUST be set to the value TBD2.

* SPI (4 octets or 8 octets) - Security Parameter Index. The new SPI.

The Critical bit MUST be 1. A value of 0 MUST be ignored.

7. IANA Considerations

This document defines two new Notify Message Types in the "IKEv2 Notify Message Types - Status Types" registry. IANA is requested to assign codepoints in this registry.

NOTIFY messages: status types	Value
OPTIMIZED_REKEY_SUPPORTED	TBD1
OPTIMIZED_REKEY	TBD2

8. Operational Considerations

Some implementations allow sending rekey messages with a different set of Traffic Selectors or cryptographic parameters in response to a configuration update. IKEv2 [RFC7296] states this SHOULD NOT be done. Whether or not optimized rekeying is used, a configuration change that changes the Traffic Selectors or cryptographic parameters MUST NOT use the optimized rekey method. It SHOULD also not use a regular rekey method but instead start an entire new IKE and Child SA negotiation with the new parameters.

9. Security Considerations

The optimized rekey removes sending unnecessary new parameters that originally would have to be validated against the original parameters. In that sense, this optimization enhances the security of the rekey process by reducing the complexity and code required.

10. Acknowledgments

Special thanks go to Valery Smyslov and Antony Antony.

11. 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>.

Authors' Addresses

Sandeep Kampati
Microsoft
India
Email: skampati@microsoft.com

Wei Pan
Huawei Technologies
101 Software Avenue, Yuhuatai District
Nanjing
Jiangsu,
China
Email: william.panwei@huawei.com

Paul Wouters
Aiven
Email: paul.wouters@aiven.io

Meduri S S Bharath
Mavenir Systems Pvt Ltd
Manyata Tech Park
Bangalore
Karnataka
India
Email: bharath.meduri@mavenir.com

Meiling Chen
China Mobile
32 Xuanwumen West Street, West District
Beijing
100053
China
Email: chenmeiling@chinamobile.com