IPsecME Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 28, 2014

Y. Nir
Check Point

August 27, 2013

Handing Over Child SAs Following Re-Authentication in IKEv2
draft-nir-ipsecme-cafr-02

Abstract

This document describes an extension to the IKEv2 protocol whereby Child SAs are moved to the new IKE SA following re-authentication. This allows for a smoother transition with no loss of connectivity.

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 http://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 February 28, 2014.

Copyright Notice

Table of Contents

1. Introduction

The Internet Key Exchange version 2 (IKEv2) protocol, as specified in [RFC5996bis] associates Child SAs with the IKE SAs under which the exchange that created them took place. With the deletion of the IKE SA due to expiry, policy change, or an explicit message from the peer, the child SAs associated with it are implicitly closed as described in section 1.4.1 of the IKEv2 document. This behavior is not desired when IKE SAs are replaced rather than deleted, because those child SAs could still be valid and there is no security reason to create new ones prematurely.

There are two cases where an IKE SA is replaced.

1. Rekeying, where new keys are generated. This is described in section 2.18 of RFC 5996. This is done mainly for key freshness.
2. Re-Authentication, where both sides authenticate, and new keys are generated. This is done as part of a risk management policy, to limit the time that compromised IKE SA keys can be used to provide the attacker access to the network. No reauthentication exchange is specified in the RFC. Instead, it's simply the Initial and Authentication exchanges done as if from scratch. This is described in section 2.8.3 of RFC 5996.

For rekeying, RFC 5996 provides a way to avoid having to re-create all child SAs. When an IKE SA is rekeyed, all the Child SAs under the old IKE SA are inherited by the new IKE SA, so that the subsequent deletion of the old IKE SA does not affect the Child SAs. This behavior is described in section 2.8 paragraph 4 of RFC 5996.

For reauthentication, RFC 5996 does not provide a similar mechanism, and section 2.8.3 explicitly says that Child SAs need to be created from scratch. This is often inconvenient, as IPsec systems usually create Child SAs only in response to traffic and multiple Child SAs may exist for a single IKE SA. The protocol extension in this draft closes this gap.

1.1. Conventions Used in This Document

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].

The terms IKE SA, Child SA, Rekeying, and Reauthentication are as described in the RFC 5996.

2. Handing Over Child SAs

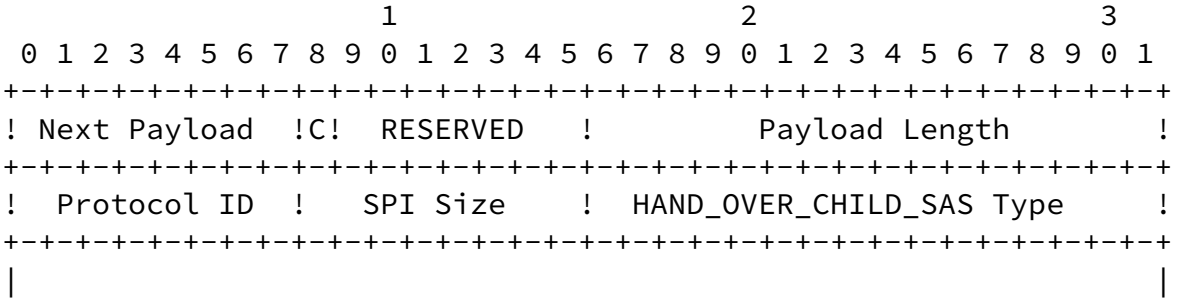
This document defines a new notification that can be sent over an old IKE SA, just after an IKE_AUTH exchange has been used to re-authenticate. The notification tells the peer to transfer all Child SAs that belong to the current (old) IKE SA to be owned by the new IKE SA, so that when the old IKE SA is deleted, those Child SAs are not. If both peers send this notification, all Child SAs belonging to the old IKE SA are immediately inherited by the new IKE SA.

In addition to the Child SAs, any IP address assigned to either peer through the use of the CFG payload (as described in section 2.19 of RFC 5996), is also associated with the new IKE SA.

The new notification MAY be accompanied by a DELETE payload, so as to transfer the Child SAs and delete the old IKE SA at the same time.

2.1. The HAND_OVER_CHILD_SAS Notification

The HAND_OVER_CHILD_SA notification is formatted as follows:



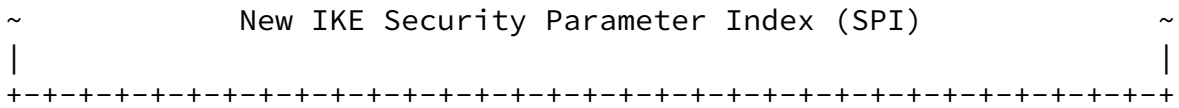


Figure 1

- Protocol ID (1 octet) MUST be zero, as specified in Section 3.10 of RFC 5996.
- SPI Size (1 octet) MUST be zero, in conformance with Section 3.10 of RFC 5996.
- HAND_OVER_CHILD_SAS Notify Message Type (2 octets) - MUST be xxxxx, the value assigned for HAND_OVER_CHILD_SAS. TBA by IANA.
- Notification Data, or New IKE Security Parameter Index (16 octets) - contains the concatenated SPIs of the new IKE SA. The Initiator SPI comes first, similar to the first 16 bytes of the IKE header. Note that this is not the SPI field of the notification payload, but the data field.

2.2. Verifying the HAND_OVER_CHILD_SAS Notification

To go through with the new IKE SA inheriting the SAs of the old IKE SA, all of the following MUST apply:

- Both sides have to be successfully authenticated, and the new IKE SA has to be established.
- The authenticated identities of both sides under the new IKE SA are the same as those under the old IKE SA. If the authenticated identity of one peer differs from the authenticated identity that it had in the previous IKE SA, the other side MUST respond with an INVALID_SYNTAX notification.
- The New IKE SPIs in the notifications from both peers MUST match bit for bit.

If the new IKE SA is not fully authenticated, or if the peer authenticated identity in the new IKE SA is not the same as in the current IKE SA, a conformant Responder MUST NOT send the HAND_OVER_CHILD_SAS Notification, and MUST not move the Child SAs.

If the Initiator has not sent the HAND_OVER_CHILD_SAS notification, but has received it in a response, it MUST ignore it and MUST NOT move the Child SAs.

If the Initiator has sent the notification, but the Responder has not sent it, then the Initiator MUST NOT move the Child SAs.

If the Initiator has sent the notification, but the notification from the Responder does not match the IKE SPIs in the Initiator's notification, the Initiator MUST send a SYNTAX_ERROR notification and MUST NOT transfer the Child SAs.

3. The Illustrated Protocol

The Informational exchange after creating a new IKE SA:

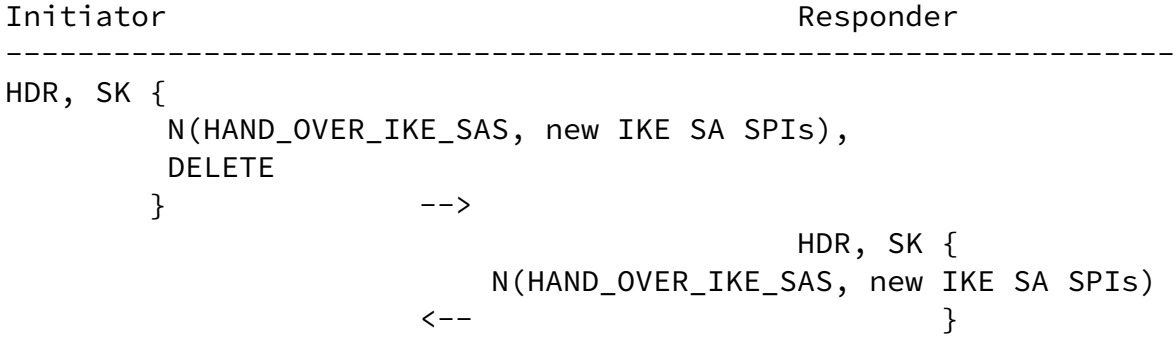


Figure 2

Note that in the above figure, the HDR has the IKE SPIs of the old IKE SAs, and the SK payload uses the keys of the old IKE SA, because this message is sent over the old IKE SA.

4. Interaction with Other Standards

This document changes things so that there is often no need to create new Child SAs along with the new IKE SA when reauthenticating. This makes the full IKE_AUTH exchange with the piggy-backed Child SA exchange (as described in RFC 5996) superfluous. Implementations should consider implementing the childless extension of IKEv2 ([RFC6023]) in addition to this specification.

5. Acknowledgements

The author would like to thank Valery Smyslov for the suggestion of moving the hand-over from the IKE_AUTH to an Informational under the old IKE SA and other suggestions. This changed (in version -01) simplified the protocol significantly.

6. IANA Considerations

IANA is requested to assign a notify message type from the status types range (16418-40959) of the "IKEv2 Notify Message Types" registry with name "HAND_OVER_CHILD_SAS"

7. Security Considerations

The HAND_OVER_CHILD_SAS notification is sent protected by the old IKE SA. This protects against stealing child SAs. The requirement for sameness of authenticated identity protects against errors by one peer transferring child SAs to some other peer, although we cannot think of any attack that would exploit this.

8. Changes from Previous Versions

[NOTE TO RFC EDITOR: PLEASE REMOVE THIS SECTION]

Version -01 moved the sending of the notification from the IKE_AUTH exchange that is part of reauthentication to the Informational exchange that is part of closing the old IKE SA. This made cryptographic binding to the old IKE SA unnecessary.

Version -02 changed the notification payload so that the IKE SPI of the other IKE SA is now in the data field of the notification payload, rather than the SPI field. This makes it more in line with how the notification payload is defined in RFC 5996.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5996bis] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", draft-kivinen-ipsecme-ikev2-rfc5996bis-00 (work in progress), August 2013.

9.2. Informative References

[RFC6023] Nir, Y., Tschofenig, H., Deng, H., and R. Singh, "A Childless Initiation of the Internet Key Exchange Version 2 (IKEv2) Security Association (SA)", RFC 6023, October 2010.

Author's Address

Yoav Nir
Check Point Software Technologies Ltd.
5 Hasolelim st.
Tel Aviv 6789735
Israel

Email: ynir@checkpoint.com