Network Working Group
Internet-Draft
Expires: August 28, 2007

J. Pezeshki
E. Ertekin
R. Jasani
C. Christou
Booz Allen Hamilton
February 24, 2007

IKEv2 Extensions to Support Header Compression over IPsec (HCoIPsec) draft-ietf-rohc-ikev2-extensions-hcoipsec-01

Status of this Memo

Copyright Notice

Abstract

When using Header Compression (HC) schemes (e.g. ROHC [ROHC]) in conjunction with IPsec [IPSEC] (i.e. [HCOIPSEC]) a mechanism is needed to negotiate ROHC configuration parameters between end-points prior to operation. Internet Key Exchange (IKE) is a mechanism which can be leveraged to handle these negotiations. This document specifies extensions to Internet Key Exchange (IKEv2 [IKEV2]) that

will allow ROHC and its associated configuration parameters to be negotiated for IPsec security associations (SAs).

Table of Contents

1. Introduction 3
2. Header Compression Channel Negotiation 3
2.1. Negotiation of Header Compression Parameters 3
2.1.1. Profiles Suboption 6
3. Security Considerations 7
4. IANA Considerations 7
5. Acknowledgments 7
6. References 8
6.1. Normative References 8
6.2. Informative References 8
Authors' Addresses 8
Intellectual Property and Copyright Statements 10

1. Introduction

Increased packet header overhead due to IPsec protection can result in inefficient utilization of bandwidth. Coupling HC with IPsec offers an efficient way to transfer protected IP traffic.

HC schemes require configuration parameters to be negotiated between the compressor and decompressor, prior to operation. Current hop-by-hop ROHC schemes negotiate these parameters through a link-layer protocol such as Point-to-Point Protocol (PPP) (i.e. ROHC over PPP [ROHCPPP]). Similarly, key exchange protocols (e.g. IKEv2) exist, which are commonly used to negotiate parameters between IPsec peers before a SA can be established. This document proposes the use of IPsec's parameter negotiation mechanism, IKE, to handle ROHC channel configuration for HCoIPsec. Various extensions to IKEv2, designed to provide this functionality, are detailed within this document.

2. Header Compression Channel Negotiation

The initialization of a ROHC session requires the negotiation of a set of configuration parameters (e.g. maximum context identifier length, etc.). As such, a mechanism must exist for a ROHC enabled device to share a list of supported HC parameters with its peer, and for the peer to select the appropriate parameters from this list.

Similarly, negotiable parameters must also be shared between IPsec peers before a SA can be established. To perform this negotiation, a key exchange protocol, IKEv2, is commonly used. IKEv2 is an extensible protocol that negotiates parameters via request/response message pairs (i.e. exchanges).

A set of extensions to IKEv2 can be defined, which will allow for ROHC parameters to be negotiated during the creation and rekeying of Child SAs. This new Notify payload will contain values for the set of ROHC parameters to be negotiated between the two ROHC peers.

2.1. Negotiation of Header Compression Parameters

ROHC configuration parameters will be negotiated at either the establishment or rekeying of a Child SA. Specifically, a Notify payload will be used during the IKE_AUTH and CREATE_CHILD_SA exchanges to negotiate the HCoIPsec session. The Notify payload sent by the initiator will contain the configuration parameters for the ROHC scheme. Upon receipt of the initiator's request, the responder will either ignore the payload (if it doesn't support ROHC or the proposed parameters) or respond with a Notify payload that contains the accepted negotiable parameters.

A new Notify Message Type value, denoted ROHC_SUPPORTED, will be added to indicate that the Notify payload is conveying ROHC channel parameters. As defined in [IPSEC], the Notify payload is specified as follows:

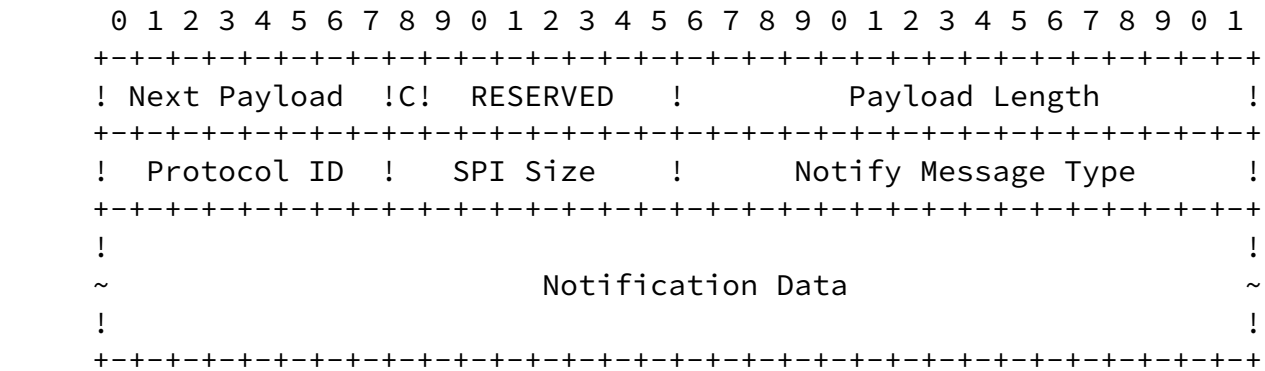


Figure 1: Notify Payload

To negotiate HCoIPsec, the values for the fields in the Notify payload are defined as follows:

Next Payload (1 octet)
Identifier for the payload type of the next payload in the message. If the current payload is the last in the message, then this field will be 0. The Next Payload value of the previous payload must be 41, indicating that this current payload is a Notify Payload.

Critical (1 bit)
   This value is set to zero, indicating that the recipient must skip this payload if it does not understand the payload type code in the Next Payload field of the previous payload.

RESERVED (7 bits)
   Must be sent as zero, and must be ignored on receipt.

Payload Length (2 octets)
   Length in octets of the current payload, including the generic payload header.

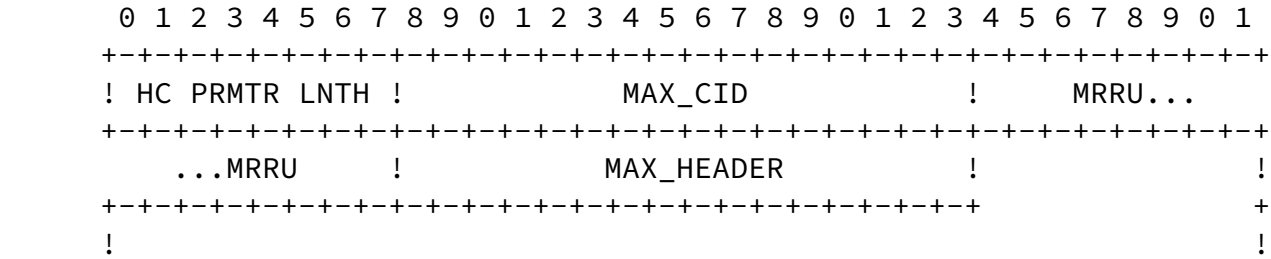
Protocol ID (1 octet)
   If this notification concerns an existing SA, this field indicates the type of that SA (i.e. IKE_SA, AH [AH], or ESP [ESP]). Since the ROHC parameters are set at SA creation, and thus do not relate to an existing SA, this field must be set to zero.

SPI Size (1 octet)

   Length in octets of the SPI as defined by the IPsec protocol ID. This value must be set to zero, since no SPI is applicable (ROHC parameters are set at SA creation, thus the SPI has not been defined).

Notify Message Type (2 octets)
   Specifies the type of notification message. This field must be set to ROHC_SUPPORTED.

ROHC configuration parameters will be communicated via a new Notify message type, denoted ROHC_SUPPORTED. The ROHC configuration parameters will be listed within the Notification Data field in the following format:



```
~                          suboptions...                        ~
!                                                               !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Notification Data field

HC PARAMETER LENGTH (1 octet)
>= 7 (i.e. the combined length of HC PARAMETER LENGTH, MAX_CID, MRRU, and MAX_HEADER)

MAX_CID (2 octets)
The MAX_CID field indicates the maximum value of a context identifier. This value must be at least 0 and at most 16383 (The value 0 implies having one context).

Suggested value: 15

Note: The value of LARGE_CIDS will be implicitly determined by this value (i.e. if MAX_CID is <= 15, LARGE_CIDS will be assumed to be 0).

MRRU (2 octets)
The MRRU field indicates the maximum reconstructed reception unit (see [ROHC], section 5.1.1).

Suggested value: 0

Note: The MRRU value is used in conjunction with the segmentation protocol defined in ROHC. Since a HCoIPsec compressor and decompressor will generally be separated by multiple link-layer "hops", segmentation will not be needed. In these cases the MRRU value should be set to zero, indicating that no segmented ROHC segmented-header packets are allowed on the channel.

MAX_HEADER (2 octets)
The largest header size in octets that may be compressed.

Suggested value: 168 octets

Note: The MAX_HEADER parameter is not used for all ROHC profiles.

If none of the ROHC profiles require this field, this value is ignored.

suboptions
The suboptions field consists of one or more suboptions. Each suboption consists of a type field, a length field and zero or more parameter octets, as defined by the suboption type. The value of the length field indicates the length of the suboption in its entirety, including the lengths of the type and length fields.

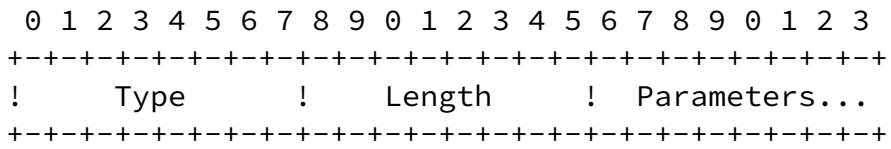


Figure 3: Suboption

Note: When a pair of SAs are created (one in each direction), the ROHC channel parameter FEEDBACK_FOR is set implicitly to the other SA of the pair (i.e. the SA pointing in the reverse direction).

2.1.1. Profiles Suboption

The set of profiles to be enabled on a Child SA is subject to negotiation.

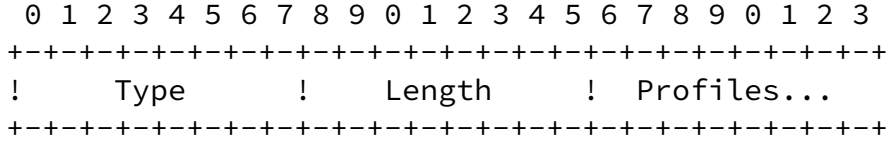


Figure 4: Profiles suboption

Type

1

Length
2n+2

Value
n octet-pairs in ascending order, each octet-pair specifying a ROHC profile supported. Values negotiated are assigned in the ROHC profile identifiers registry [ROHCPROF].

3. Security Considerations

The negotiated HC schemes and parameters negotiated via IKEv2 do not add any new vulnerabilities beyond those associated with the normal operation of IKEv2.

4. IANA Considerations

This document defines a new Notify Message Type. Therefore, if the proposal is accepted, IANA is requested to allocate on value from the IKEv2 Notify Message Types registry to indicate ROHC_SUPPORTED.

5. Acknowledgments

The authors would like to thank Mr. Sean O'Keeffe, Mr. James Kohler, and Ms. Linda Noone of the Department of Defense, as well as Mr. Rich Espy of OPnet for their contributions and support in the development of this document. The authors would also like to thank Mr. Tero Kivinen for providing his technical expertise for this document. In addition, the authors would like to thank the following for their numerous reviews and comments to this document:

Dr. Stephen Kent
Dr. Carsten Bormann
Mr. Lars-Erik Jonnson

Finally, the authors would also like to thank Mr. Tom Conkle, Ms.

Michele Casey, and Mr. Etzel Brower.

6. References

6.1. Normative References

[ROHC] Bormann, C., Burmeister, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., Yoshimura, T., and H. Zheng, "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", RFC 3095, July 2001.

[IPSEC] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[HCOIPSEC] Ertekin, E., Christou, C., and R. Jasani, "Integration of Header Compression over IPsec Security Associations", work in progress , February 2007.

[IKEV2] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[ROHCPROF] "RObust Header Compression (ROHC) Profile Identifiers", www.iana.org/assignments/ROHC-pro-ids , October 2005.

6.2. Informative References

[ROHCPPP] Bormann, C., "Robust Header Compression (ROHC) over PPP", RFC 3241, April 2002.

[AH] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[ESP] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

Authors' Addresses

Jonah Pezeshki
Booz Allen Hamilton
13200 Woodland Park Dr.
Herndon, VA 20171
US

Email: pezeshki_jonah@bah.com

Emre Ertekin
Booz Allen Hamilton
13200 Woodland Park Dr.
Herndon, VA 20171
US

Email: ertekin_emre@bah.com

Rohan Jasani
Booz Allen Hamilton
13200 Woodland Park Dr.
Herndon, VA 20171
US

Email: jasani_rohan@bah.com

Chris Christou
Booz Allen Hamilton
13200 Woodland Park Dr.
Herndon, VA 20171
US

Email: christou_chris@bah.com

Full Copyright Statement

Intellectual Property

ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).