Network Working Group	E. Ertekin
Internet-Draft	C. Christou
Expires: April 17, 2009	R. Jasani
	J. Pezeshki
	Booz Allen Hamilton
	October 14, 2008

TOC

IKEv2 Extensions to Support Robust Header Compression over IPsec (ROHCoIPsec)
draft-ietf-rohc-ikev2-extensions-hcoipsec-07

Status of this Memo

Abstract

In order to integrate ROHC with IPsec [ROHCOIPSEC], a mechanism is needed to negotiate ROHC configuration parameters between end-points. Internet Key Exchange (IKE) is a mechanism which can be leveraged to handle these negotiations. This document specifies extensions to IKEv2 [IKEV2] that will allow ROHC and its associated configuration parameters to be negotiated for IPsec security associations (SAs).

Table of Contents

---

1. Introduction

TOC

Increased packet header overhead due to IPsec [IPSEC] can result in the inefficient utilization of bandwidth. Coupling ROHC [ROHC] with IPsec offers an efficient way to transfer protected IP traffic.
The operation of ROHCoIPsec [ROHCOIPSEC] requires configuration parameters to be negotiated between the compressor and decompressor. Current specifications for hop-by-hop ROHC negotiate these parameters through a link-layer protocol such as Point-to-Point Protocol (PPP) (i.e. ROHC over PPP [ROHCPPP]). Since key exchange protocols (e.g. IKEv2) can be used to negotiate parameters between IPsec peers, this document defines extensions to IKEv2 to negotiate ROHC parameters for ROHCoIPsec.

---

2. ROHC Channel Negotiation

TOC

The initialization of a ROHC session requires the negotiation of a set of configuration parameters (e.g. MAX_CID, PROFILES, etc.). The following subsections define extensions to IKEv2 which enables an initiator to propose a set of ROHC parameters; the responder selects the appropriate parameters from this list, and responds with the accepted parameters for the ROHC channel.

2.1. Negotiation of ROHC Channel Parameters

TOC

ROHC configuration parameters will be negotiated at either the establishment or rekeying of a Child SA. Specifically, a new Notify message type is used during the IKE_AUTH and CREATE_CHILD_SA exchanges to negotiate these parameters.

The Notify payload sent by the initiator contains the configuration parameters for the ROHC implementation. 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 ROHC channel parameters. The accepted parameters are an intersection between the parameters proposed by the initiator and the parameters supported by the responder (e.g. if the initiator proposes a MAX_CID value of 15, but the responder only supports a MAX_CID value of 13, the responder will respond with a value of 13, which is supported by both parties).
Note that only one Notify payload is used to convey ROHC parameters per exchange. If multiple Notify payloads relaying ROHC parameters are received by the responder, all but the first such Notify payload must be dropped. If the initiator does not receive a Notify Payload with the responder's accepted ROHC channel parameters, ROHC must not be enabled on the Child SA.
A new Notify Message Type value, denoted ROHC_SUPPORTED, will indicate that the Notify payload is conveying ROHC channel parameters. The Notify Payload (as defined in [IKEV2]) is illustrated in Figure 1 below:

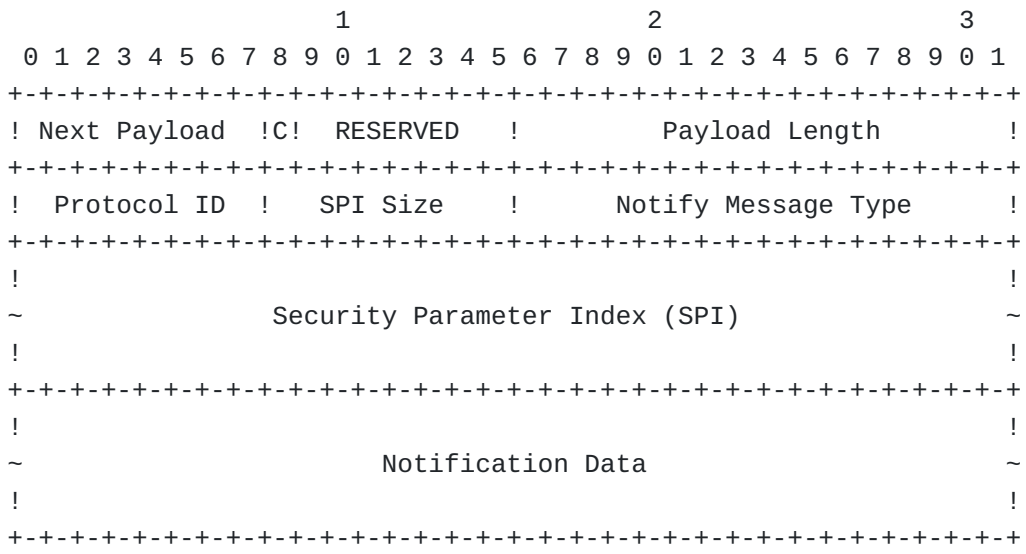

Figure 1. Notify Payload format.

The fields of the Notify Payload are set as follows:
Next Payload (1 octet)

> Identifier for the payload type of the next payload in the message. Further details can be found in [IKEV2].

Critical (1 bit)

> Since all IKEv2 implementations must support the Notify Payload, this value is zero.

Protocol ID (1 octet)

> Since this Notification message is used during the creation of a Child SA, this field must be set to zero.

SPI Size (1 octet)

> 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)

> 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 of the Notify payload in the following format (default values for the configuration parameters are consistent with [ROHCPPP]):

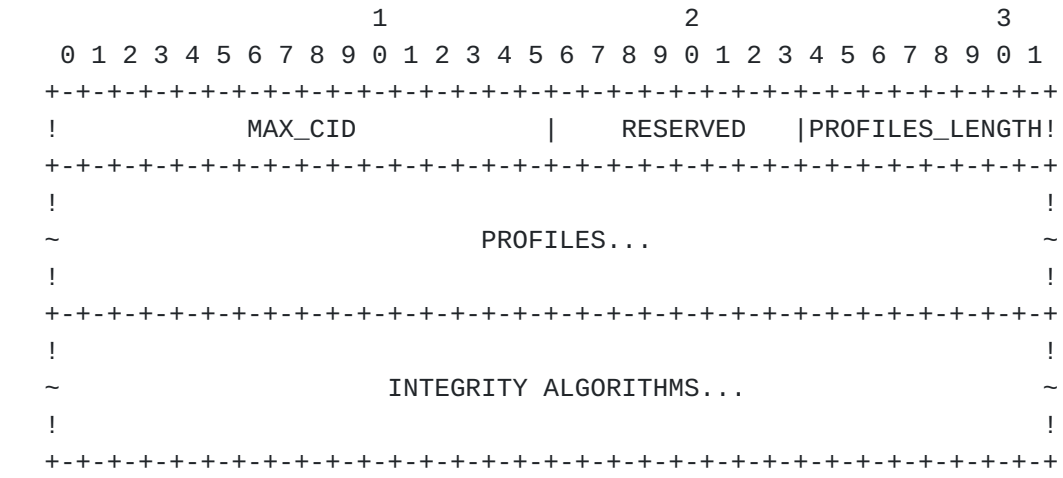

Figure 2. Notification Data field for the ROHC_SUPPORTED Notify message type.

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

PROFILES_LENGTH (1 octet)

> The total number of profiles contained within the PROFILES field (note that each ROHC profile is 2-octets in length).

PROFILES (variable)

> The set of profiles to be enabled for the ROHC process. Profiles are further detailed in [ROHC]. In addition, several common profiles are defined in [ROHCPROF]. These 16-bit profile identifiers are to be sent in network byte order.

INTEGRITY ALGORITHMS

> The set of Integrity Algorithms that may be use to ensure the integrity of the decompressed packets (i.e. ensure that the packet headers are properly decompressed). Each Integrity Algorithm is represented by a 2-octet value that corresponds to the value listed in [IKEV2-PARA] "For Transform Type 3 (Integrity Algorithm)" section.
>
> It is noted that:
>
> 1. The length of this field is inferred from the Notify Payload's "Payload Length" field.
>
> 2. The key for this Integrity Algorithm is computed using the same method as is used to compute IPsec's Integrity Algorithm key ([IKEV2], Section 2.17).
>
> 3. A ROHCoIPsec implementation may choose to negotiate a value of "0" in this field (i.e., NONE, as defined in the Integrity Algorithm Transform ID registry).

The negotiated set of ROHC parameters are associated with the inbound/ outbound pair of SAs established by each IKEv2 CREATE_CHILD_SA exchange.
The following ROHC channel parameters are not negotiated:

*LARGE_CIDS: This value is implicitly determined by the value of MAX_CID (e.g. if MAX_CID is <= 15, LARGE_CIDS is assumed to be 0).

*MRRU: IPsec implementations will always implement path MTU discovery; therefore, ROHC packets will never need to use ROHC segmentation over an IPsec SA. As a result, this value will always be zero, and does not need to be negotiated.

*FEEDBACK_FOR: 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).

3. Security Considerations

TOC

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

4. IANA Considerations

TOC

This document defines a new Notify Message (Status Type). Therefore, IANA is requested to allocate one value from the IKEv2 Notify Message registry to indicate ROHC_SUPPORTED. Note that, since this Notify Message is a Status Type, values ranging from 0 to 16383 must not be allocated for ROHC_SUPPORTED.

5. Acknowledgments

TOC

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

*Mr. Pasi Eronen

*Dr. Joseph Touch

*Mr. Yoav Nir

Finally, the authors would also like to thank Mr. Tom Conkle, Ms. Michele Casey, and Mr. Etzel Brower.

6. References

TOC

6.1. Normative References

TOC

[ROHCOIPSEC]	Ertekin, E., Christou, C., and R. Jasani, “Integration of Robust Header Compression over IPsec Security Associations,” work in progress , October 2008.
[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.
[IKEV2]	Kaufman, C., “Internet Key Exchange (IKEv2) Protocol,” RFC 4306, December 2005.
[ROHCPPP]	Bormann, C., “Robust Header Compression (ROHC) over PPP,” RFC 3241, April 2002.

6.2. Informative References

TOC

[ROHCPROF]	Pelletier, G. and K. Sandlund, “RObust Header Compression Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP and UDP Lite,” www.iana.org/assignments/ROHC-pro-ids , May 2007.
[IKEV2-PARA]	IANA, “IKEv2 Parameters, http://www.iana.org/assignments/ikev2-parameters,” January 2008.

Authors' Addresses

TOC

	Emre Ertekin
	Booz Allen Hamilton
	13200 Woodland Park Dr.
	Herndon, VA 20171
	US
Email:	ertekin_emre@bah.com
	Chris Christou
	Booz Allen Hamilton

	13200 Woodland Park Dr.
	Herndon, VA 20171
	US
Email:	christou_chris@bah.com
	Rohan Jasani
	Booz Allen Hamilton
	13200 Woodland Park Dr.
	Herndon, VA 20171
	US
Email:	jasani_rohan@bah.com
	Jonah Pezeshki
	Booz Allen Hamilton
	13200 Woodland Park Dr.
	Herndon, VA 20171
	US
Email:	pezeshki_jonah@bah.com

Full Copyright Statement

TOC

Intellectual Property

such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.