6Lo Working Group S. Raza
Internet-Draft S. Duquennoy
Intended Status: Standard Track SICS, Stockholm
G. Selander
Ericsson, Stockholm
Expires: September 26, 2014 March 25, 2014

Compression of IPsec AH and ESP Headers for Constrained Environments
draft-raza-6lo-ipsec-00

Abstract

This document describes the header compression mechanisms for the IPsec [RFC4301] based on the encoding scheme standardized in [RFC6282]. The IPsec Authentication Header (AH) and Encapsulated Security Payload (ESP) headers are compressed using Next Header Compression (NHC) defined in [RFC6282]. This document does not invalidate any encoding schemes proposed in 6LoWPAN [RFC6282] but rather complements it with compressed IPsec using the free bits in the IPv6 Extension Header encoding.

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 September 26, 2014.

Copyright and License Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1 Introduction

[RFC6282] defines how IPv6 datagrams can be routed over IEEE 802.15.4 [IEEE802.15.4]-based networks. [RFC6282] defines a header compression schemes that can significantly reduce the size of IP, IP extension, and UDP headers. This enables the routing of heavy-weight IP traffic to resource-constrained [IEEE802.15.4]-based wireless network. The security in [IEEE802.15.4]-based IP network or what is more commonly known 6LoWPAN networks is particularly important as we connect the insecure Internet with the vulnerable wireless network. The standardized and mandatory security solution for IPv6 is IP security (IPsec) [RFC4301]. This means that every IPv6 host on Internet is able to process IP packets secured with IPsec. IPsec, in transport mode, can provide end-to-end (E2E)secure communication between the two hosts in the IP network. Thus, it is beneficial to extend 6LoWPAN so that IPsec communication between an IPv6 device (e.g. a sensor node) in 6LoWPAN and IPv6 nodes on conventional Internet becomes possible. This document does not cover the tunnel mode of IPsec.

With IPv6 architecture it is possible to protect ICMPv6 messages, using IPsec. As the RPL Control Message [RFC6550] is an ICMPv6 message, it is therefore possible to protect it with IPsec. However, all RPL Control Message, except DAO / DAO-ACK messages in non-storing mode, are exchanged between two neighboring devices and have the scope of a link. Though IPsec security associations can be created between two neighboring devices, IEEE 802.15.4 security at the link layer is more suitable for per-hop protection, and IPsec in transport mode can be used to protect DAO/DAO-ACK messages in non-storing mode.

It is desirable to complement 6LoWPAN header compression with IPsec to keep packet sizes reasonable in resource constrained [IEEE802.15.4]-based network. There are no header compression specified for IPsec's AH[RFC4302] and ESP[RFC4303] extension headers. This draft therefore proposes AH and ESP extension header encoding schemes.

1.1 Terminology

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 RFC 2119 [RFC2119].

2. Linking IPsec Headers Compression with 6LoWPAN

[RFC6282] defines the general format of NHC that can be used to encode IP extension headers. [RFC6282] already defines an NHC encoding for IPv6 Extension Headers (NHC_EH) that can be used to link uncompressed AH and ESP headers to the 6LoWPAN header compression. In order to compress the IP extension headers a GHC byte for Extension Header (GHC_EH) [draft-bormann-6lo-ghc-00] is proposed which has the same layout as NHC_EH with different ID bits. NHC_EH and GHC_EH consist of an octet where three bits (bits 4, 5 and 6) are used to encode the IPv6 Extension Header ID (EID). Out of eight possible values for the EID, six are assigned and the remaining two slots (101 and 110) are currently unassigned. As AH and ESP are IP extension headers it makes sense to use one of these unassigned slots for the IPsec headers. We propose to use the reserved slot 101 for the IPsec headers, AH or ESP. The corresponding ID field in the AH or ESP will distinguish these headers from each other. It is also necessary to set the NH bit in NHC_EH or GHC_EH to 1 to specify that the next header (a header after AH or ESP, e.g. UDP) is NHC-encoded.

3. LOWPAN_NHC for Authentication Header

6LoWPAN can be used to compress a significant number of bits in AH. The next header is decided based on the value of NH bit in the IPv6 Extension Header Encoding in [RFC6282]. This draft proposes to always elide the length field. The payload length field (the length of AH header in 32-bit words units minus "2" [RFC4302]) in the AH header is always elided, as it can be inferred from the lower layers: either from the IEEE 802.15.4 header or the 6LoWPAN header. The size of ICV can be obtained from the SPI value because the length of the authenticating data depend on the algorithm used and are fixed for any input size. The RESERVED field in the AH header is also always elided. The SPI and SN are compressed using the proposed NHC encoding for the AH header shown in Figure 1 and are explained below.

```
  0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
| 1 | 1 | 0 | 1 |  SPI  |  SN   |
+---+---+---+---+---+---+---+---+
```

Figure 1: Proposed LOWPAN NHC encoding for AH

- o The first four bits in the NHC AH represent the NHC ID we define for AH. These are set to 1101.

- o If SPI = 00: the default SPI for the IEEE 802.15.4 network is used and the SPI field is omitted. We set the default SPI value to 1. This does not mean that all nodes use the same security association (SA), but that every node has a single preferred SA, identified by SPI 1. If SPI = 01: the least significant 8 bits of the SPI are carried inline; the remaining 24 bits are elided. If

SPI = 10: the least significant 16 bits of the SPI are carried inline; the remaining 16 bits are elided. If SPI = 11: All 32 bits of the SPI are carried inline.

- If SN = 00: the least significant 8 bits of sequence number are carried inline. The remaining bits are elided. If SN = 01: the least significant 16 bits of the SN are carried inline; the remaining 16 bits are elided. If SPI = 10: the least significant 24 bits of the SPI are carried inline; the remaining 8 bits are elided. If SPI = 11: All 32 bits of the SPI are carried inline.

  The sequence number field in the AH header [RFC4302] contains a value 1 for the first packet sent using a given Security Association (SA), and it is incremented sequentially for the subsequent packets. Note that by using 8-bit sequence number we do not limit the size of sequence number to 255, but propose to use 8 bits for the sequence number prior to the transmission of the 256th packet on an SA. From the 2^8 to 2^(16-1) we propose to use 16-bit sequence number. Follow the same procedure for the 24-bit sequence number as well. However, the sender and the receiver sequence number counters must be reset prior to sending 2^32nd packet as proposed in [RFC4302].

Note that even when used in 6LoWPAN, AH calculates the ICV on the uncompressed IP header, thus allowing authenticated communication with Internet hosts. The minimum length of a standard AH, supporting the mandatory HMAC-SHA1-96[RFC4835], consists of 12 bytes of header fields plus 12 bytes of ICV. Figure 2 shows a sample NHC compressed IP/UDP packet secured with AH. Using NHC encoding for the AH we can reduce the AH header overhead from 24 bytes to 14 bytes: 1 byte of next header, 1 byte of length, 2 bytes of Reserved field, 4 bytes of SPI, and 2 bytes of sequence number. However, two additional bytes are used to define NHC_EH and NHC_AH. Therefore, in the best case, with AES-XCBC-MAC-96[RFC3566] or HMAC-SHA1-96 ciphers (when 12 bytes are used for ICV), applying NHC encoding for AH saves 8 bytes in each data packet secured with IPsec AH.

```
|   octet 1      |  octet 2      |    octet 1    |    octet 1    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         LOWPAN_IPHC            | Hop Limit     | Source Address|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Source Address|      Destination Address       | LOWPAN_NHC_EH |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| LOWPAN_NHC_AH |       Sequence Number          |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+              +
|                                                                |
|         Integrity Check Value-ICV (Variable)  +-+-+-+-+-+-+-+-+
|                                                | LOWPAN_NHC_UDP|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Source Port   | Dest Port     |    Checksum    |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+              +
|                                                                |
+                                                                +
|                   UDP Payload (Variable)                       |
+                                                                +
|                                                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: A sample NHC compressed IP/UDP packet secured with AH.

4. LOWPAN_NHC for Encapsulated Security Payload (ESP)

The encryption in the IPsec ESP includes Payload Data, Padding, Pad Length and Next Header fields in the ESP. Therefore, we cannot compress these fields at the 6LoWPAN layer, and these fields are always carried inline. Also, when using ESP the UDP header and payload is also encrypted, hence cannot be compressed using NHC encodings for UDP defined in the [RFC6282]. However, we can compress the SPI and and sequence number (SN) fields in the ESP header. Figure 3 shows a proposed NHC encodings for the ESP that are explained below.

```
  0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
| 1 | 1 | 1 | 0 |  SPI  |  SN   |
+---+---+---+---+---+---+---+---+
```

Figure 3: Proposed LOWPAN NHC encoding for ESP

- o The first four bits in the NHC ESP represent the NHC ID we define for ESP. These are set to 1110.

- o The SPI and SN bits are encoded exactly the same way as in

Section 3 for the AH header.

In case of ESP we cannot skip the next header unless the end hosts are able to execute 6LoWPAN compression/decompression and encryption/decryption jointly. The nodes in the 6LoWPAN network make their decision about the next header based on the NH value not the actual header that is carried inline. In the case of ESP we MUST set the NH value in the NHC_EH or GHC_EH to zero to indicate that the full 8 bits of next header field are carried inline.

```
|   octet 1      |   octet 2      |    octet 1     |    octet 1     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          LOWPAN_IPHC            |  Hop Limit     | Source Address|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Source Address|      Destination Address         | LOWPAN_NHC_EH |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| LOWPAN_NHC_ESP|        Sequence Number           |       IV       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Initialization Vector (Variable Size)         |  Source Port   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Source Port  |      Destination Port            |     Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Length      |          Checksum                |                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                 +
|                     UDP Payload (Variable)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Pad                |  Pad Length    |  Next Header   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                                   |
+                                                                   +
|                Integrity Check Value (Variable)                   |
+                                                                   +
|                                                                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: A sample NHC compressed IP/UDP packet secured with ESP.

With perfect block alignment, the minimum ESP overhead without authentication is 10 bytes [RFC4303]. After optimal compression this header overhead is reduced to 6 bytes, considering that two bytes are used for NHC_EH and NHC_ESP. ESP also includes an IV which is equal to the size of an encryption block; 16 bytes in the case of AES. If authentication is enabled in the ESP, additional 12 bytes of ICV are also required. Figure 4 shows an UDP/IP packet secured with compressed ESP.

5. Implementation Considerations

We provide an open source implementation of the proposed compression scheme in the Contiki operating system. The implementation is released under BSD license and can be obtained through the contikiprojects repository at the following URI: svn://svn.code.sf.net/p/contikiprojects/code/sics.se/ipsec

6. Security Considerations

The compression scheme proposed in this document does not compromise any of the security provided by IPsec AH and ESP. In particular, the SN field is compressed in an on-demand fashion, as described in Section 3. In order to overcome replay attacks, it is recommended that the communication end-points should re-establish a security association before the sequence number overflows. However, in constrained environments, different implementations can decide the overflow size; 2^8, 2^16, 2^24, or 2^32. This leads to a trade-off between the overhead incurred by establishing a new security association and by sending more bits of sequence number. The Initialization Vector (IV) and Integrity Check Value (ICV) are also not compressed to take full advantage of IPsec AH and ESP security.

7. IANA Considerations

[RFC6282] creates a new IANA registry for the LOWPAN_NHC header type where the two slots, 1110101N and 1110110N, in LOWPAN_NHC for the IPv6 Extension Header are unassigned. This document requests the assignment of one of these two unassigned values, 1110101N, to IPsec AH and ESP. This document also requests the assignment of following contents:

1101XXYY: The 6LOWPAN_NHC encoding for the IPsec Authentication Header.

1110XXYY: The 6LOWPAN_NHC encoding for the IPsec Encapsulated Security Payload Header.

Capital letters in bit positions represent class-specific bit assignments. The letters XX and YY represent SPI and SN respectively, as defined in Section 3.

8. Acknowledgements

The work is funded by CALIPSO, Connect All IP-based Smart Objects, funded by the European Commission under FP7 with contract number FP7-ICT-2011.1.3-288879.

9. References

9.1. Normative References

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

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC6282] Hui, J., Ed., and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, September 2011.

[RFC4303] J. Hui, P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, September 2011

9.2. Informative References

[RFC3566] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.

[RFC4835] Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, April 2007.

Authors' Addresses

Shahid Raza
SICS Swedish ICT AB (SICS)
Isafjordsgatan 22, 16440 Kista
SWEDEN

Phone: +46-(0)768831797
EMail: shahid@sics.se

Simon Duquennoy

SICS Swedish ICT AB (SICS)
Isafjordsgatan 22, 16440 Kista
SWEDEN

Phone: +46-(0)702021482
EMail: simonduq@sics.se

Goeran Selander
Ericsson
Farogatan 6, 16480 Kista
SWEDEN

Email: goran.selander@ericsson.com