Compression of IPsec AH and ESP Headers for Constrained Environments
draft-raza-6lo-ipsec-04

{shahid.raza, simon.duquennoy}@sics.se
goran.selandaer@ericsson.com
Status of the Document

• First submitted as a position paper to the Smart Object Workshop [RFC6574] co-located with IETF 80.
• Later submitted to 6LoWPAN WG
• Moved to 6lo and included in the 6lo BoF
• Presented in 6lo during the IETF93
• Presented in 6lo during the IETF94
Salient Features

• Does not require any modification in the IPsec standard
  – End-to-End compatible with any IPsec enabled hosted on the Internet.
  – Only performs header compression within 6LoWPAN networks without compromising any security properties

• Seamlessly links with the 6LoWPAN standard

• Other compression mechanisms exists
  – draft-mgl-t-6lo-diet-esp-01 requires changes in the IPsec standard and should also be supported/enabled in hosts on the Internet
  – ROHC [RFC5795][RFC5856]) also targets any Internet hosts and not specific to 6LoWPAN networks
  – Both are complementary to our solution
IETF94 Comments

• AH is almost not used today; why should we include it in this draft?
  – A paragraph is added in the introduction section on the use of AH in the IoT.

• Why the proposed ESP NHC ID-bits are taken from the IANA’s assigned bit?
  – One of the free ID-bits are now used.

• Use only one EID reserve bit and make the other bit extensible.
  – Done

• Why not to use CCM?
  – This draft does not recommend or mandates any specific cipher suites; it only compresses the headers.
IP Security (IPsec)

• **End-to-end Security at the Network layer**
  - Part of the OS
  - Protects IP and UDP/TCP headers
  - IPsec Transport mode for the Internet of Things

• **Authentication Header (AH) [RFC-4302]**
  - Integrity and authentication

• **Encapsulated Security Payload (ESP) [RFC-4303]**
  - Confidentiality and optionally integrity and authentication

• **AH and ESP are *IP extension headers* **

• IPv6 nodes SHOULD implement IPsec [RFC 6434]
Linking IPsec Headers Compression with 6LoWPAN

IP Header Compression (IPHC) [RFC-6282]

BIT 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 1 1 TF NH NLIM CID SAC SAM M DAC DAM

IPv6 Header | IPv6 Extension Headers | UDP | UDP Payload
Linking IPsec Headers Compression with 6LoWPAN

IP Header Compression (IPHC) [RFC-6282]

<table>
<thead>
<tr>
<th>BIT</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>TF</td>
<td>NH</td>
<td>NLIM</td>
<td>CID</td>
<td>SAC</td>
<td>SAM</td>
<td>M</td>
<td>DAC</td>
<td>DAM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IPv6 Header | IPv6 Extension Headers | UDP | UDP Payload

Variable Length NHC ID | Compressed next header

Next Header Compression (NHC) [RFC-6282]
Linking IPsec Headers Compression with 6LoWPAN

IP Header Compression (IPHC) [RFC-6282]

IPv6 Header | IPv6 Extension Headers | UDP | UDP Payload

Variable Length NHC ID | Compressed next header

Next Header Compression (NHC) [RFC-6282]
Linking IPsec Headers Compression with 6LoWPAN

IP Header Compression (IPHC) [RFC-6282]

IPv6 Header | IPv6 Extension Headers | UDP | UDP Payload

Next Header Compression (NHC) [RFC-6282]
Proposal 1 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved -
6: Reserved -
7: IPv6 Header
Linking IPsec Headers Compression with 6LoWPAN (cont...)

Proposal 1 - IPv6 EID:

- 0: IPv6 Hop-by-Hop Options Header
- 1: IPv6 Routing Header
- 2: IPv6 Fragment Header
- 3: IPv6 Destination Options Header
- 4: IPv6 Mobility Header
- 5: Reserved -
- 6: Reserved -
- 7: IPv6 Header

**Extension Header Order [RFC2460]**
- IPv6 header
- Hop-by-Hop Options header
- Destination Options header
- Routing header
- Fragment header
- Authentication header
- Encapsulating Security Payload header
- Destination Options header
- upper-layer header
Linking IPsec Headers Compression with 6LoWPAN (cont...)

Proposal 1 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved - IPv6 Authentication Header
6: Reserved - IPv6 Encapsulated Security Payload
7: IPv6 Header
Linking IPsec Headers Compression with 6LoWPAN (cont...)

<table>
<thead>
<tr>
<th>BIT</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOWPAN_NHC_EH</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>EID</td>
<td>NH</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Proposal 1 - IPv6 EID:**

- 0: IPv6 Hop-by-Hop Options Header
- 1: IPv6 Routing Header
- 2: IPv6 Fragment Header
- 3: IPv6 Destination Options Header
- 4: IPv6 Mobility Header
- 5: Reserved - IPv6 Authentication Header
- 6: Reserved - IPv6 Encapsulated Security Payload
- 7: IPv6 Header

**Proposal 2 - IPv6 EID:**

- 0: IPv6 Hop-by-Hop Options Header
- 1: IPv6 Routing Header
- 2: IPv6 Fragment Header
- 3: IPv6 Destination Options Header
- 4: IPv6 Mobility Header
- 5: Reserved
- 7: IPv6 Header

* Variable length NHC ID is used to distinguish AH and ESP
Linking IPsec Headers Compression with 6LoWPAN (cont...)

Proposal 1 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved
6: *Reserved
7: IPv6 Header

Proposal 2 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved
6: *Reserved
   IPv6 Authentication Header
   & IPv6 Encapsulated Security Payload
7: IPv6 Header

* Variable length NHC ID is used to distinguish AH and ESP
Compressing IPsec (cont...)

- Proposed LOWPAN NHC encoding for AH

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

- Proposed LOWPAN NHC encoding for ESP

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

- SPI: Security Parameter Index
- SN: Sequence Number
Compressing IPsec (cont...)

- Proposed LOWPAN NHC encoding for AH

- Proposed LOWPAN NHC encoding for ESP

- SPI: Security Parameter Index
- SN: Sequence Number
Compressed IPsec AH

IP Datagram secured with AH

Compressed IP Datagram secured with compressed AH
IPsec vs. IEEE 802.15.4 security

- Multi hops with 512 byte data size with AES CCM

Questions/Comments

shahid@sics.se

Source Code
svn co https://contikiprojects.svn.sourceforge.net/svnroot/contikiprojects/sics.se/ipsec ipsec