PROPOSED IMPROVEMENTS TO ESP AIDING DATA CENTER DEPLOYMENTS

Michael Rossberg · Michael Pfeiffer
Technische Universität Ilmenau, Germany
Motivation

• Scenario: ESP as is in data centers

• Due to handling of sequence numbers:
  • Limited parallelism
  • No multicast replay protection
  • Issues with QoS

• Due to trailer: complex protocol handling
  • Fragments
  • Segments
  • Alignment

→ Approach: change ESP a “little” → New protocol/version/mode?
Packet Layout for Tunnel Mode

Security Parameter Index (SPI)
Sequence Number
Initialization Vector
Encapsulated Packet
Padding (0-3 byte) Pad. Len. Next Hdr.
Integrity Check Value (ICV)

Security Parameter Index (SPI)
Sender ID Window ID
Sequence Number
Integrity Check Value (ICV)
Encapsulated Packet

Proposed Protocol Changes
Resulting Packet Layout for Tunnel Mode

- Multiple replay windows per SA
  - Allows scaling over CPU cores,
  - Multicast replay protection &
  - Replay window per QoS class
- Full 64-bit sequence counter
- No trailer required
- Implicit padding if required
- No AAD required

Could be negotiated during IKE & coexist

<table>
<thead>
<tr>
<th>Security Parameter Index (SPI)</th>
<th>Used as IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender ID</td>
<td>Window ID</td>
</tr>
<tr>
<td>Sequence Number</td>
<td></td>
</tr>
<tr>
<td>Integrity Check Value (ICV)</td>
<td></td>
</tr>
<tr>
<td>Encapsulated Packet</td>
<td>Auth. &amp; Enc.</td>
</tr>
</tbody>
</table>
THANKS FOR LISTENING!

Contact:

michael.rossberg@tu-ilmenau.de & michael.pfeiffer@tu-ilmenau.de

Further details:

Parallel ESP processing: Threading model

- "Black" interface
  - TX queues
  - RX queue
  - Encryption threads
  - Single RSS thread

- "Red" interface
  - RX queues
  - TX queues
  - Red RX threads
  - Red TX threads

- IPsec en-/decryption
  - Single SeqNo thread
  - Decryption threads

The diagram illustrates the threading model for processing ESP (Encapsulating Security Payload) in a network context, distinguishing between "Black" and "Red" interfaces.
Non-parallel “well-behaved” throughput

- **64 Byte Packets**
  - ESP (DPDK): 2.0 Gbit/s
  - ESP (prototype): 2.0 Gbit/s
  - VPE: 2.0 Gbit/s

- **1420 Byte Packets**
  - ESP (DPDK): 17.5 Gbit/s
  - ESP (prototype): 20.0 Gbit/s
  - VPE: 20.0 Gbit/s
Processing Time vs. Packet Size

- ESP
- VPE

Packet size [Byte]

Time to encrypt $10^7$ packets [s]

- 0
- 2
- 4
- 6
- 8
- 10
- 12
Processing Time vs. Additional Headroom

![Graph showing Processing Time vs. Additional Headroom]

- Time to encrypt $10^7$ packets [s]
- Extra Headroom [Bytes]

Legend:
- VPE
- ESP